Department for Transport

SECURITY GUIDANCE
ON THE CARRIAGE OF DANGEROUS GOODS BY ROAD AND RAIL

REGULATIONS 5, 7 & 8 OF THE CARRIAGE OF DANGEROUS GOODS AND USE OF TRANSPORTABLE PRESSURE EQUIPMENT REGULATIONS (CDGUTPE) 2009 AS AMENDED

Published by

Department for Transport
Great Minster House
33 Horseferry Road
London SW1P 4DR
020 7944 8300
www.gov.uk

Department for Transport
Great Minster House
33 Horseferry Road
London SW1P 4DR
Telephone 0300 330 3000
General enquiries https://forms.dft.gov.uk
Website www.gov.uk/dft

Contents

Table of Updates

Updated by	Date of update	Section updated	Next review due
Land Transport Security	February 2016	Full document update	2017

SECTION 1: INTRODUCTION

The Department has produced this guidance document to help organisations such as carriers and consignors with the secure transport of dangerous goods. This includes helping small or new enterprises with limited security experience to deliver security measures applicable to their transport operation and help demonstrate that any relevant or mandatory security requirements of Chapter 1.10 of the ADR and RID Regulations are being met.

Using this guidance, along with other industry and Government produced information, will not only help your organisation protect itself from a range of threats, including acts of terrorism or sabotage, but also contribute to the wider efforts to improve security and resilience in the transport sectors.

The guidance contained in this document, including the contents of the annexes, is not totally prescriptive or exhaustive. It is offered without prejudice to the absolute duty of duty holders to comply with the regulations, adoption of the guidance may not necessarily be accepted by the relevant regulator as equating with compliance in all cases and as such, duty holders have the right to adopt alternative means of securing compliance. Each organisation should make its own judgement as to which measures apply to ensure the appropriate requirements are met. Organisations should determine which and how far to apply those measures according to their operation. Security should be an integral part of the quality and management systems of every organisation involved in the carriage of dangerous goods.

Regulatory background

Following the terrorist attacks in the USA on 11 September 2001 and other terrorist incidents, it was considered necessary to implement security measures to increase the security of dangerous goods carried by road and rail. Security provisions are now established in Chapter 1.10 of the ADR and RID Regulations and address all parties involved in the transport chain. In Great Britain, these security provisions apply through the Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations (CDGUTPE) 2009 (as amended). Chapter 1.10 forms the basis of the Land Transport Security Division, Department for Transport's security compliance programme. Any variations which arise through British derogations are in a DfT approved document which can be found at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/3275/approved-derogations-transitional-provisions.pdf

The Northern Ireland Health and Safety Executive is responsible for implementation in Northern Ireland which has a separate security regime and applies its own regulations. Those regulations apply the same international modal provisions by virtue of the same EU Directive.

Ministerial responsibility for the secure transport of dangerous goods rests with the Department for Transport with the exception of Class 7 (radioactive material) which falls to the Office for Nuclear Regulation (ONR). Specific advice on the secure carriage of radioactive material should be obtained from the ONR, their contact details can be found in Annex 8 of this document.

Security Measures

Dangerous Goods are assigned to one of nine classes according to the hazard or most predominant of the hazards they present and the classes are further sub-divided into divisions. The classes are:

Class 1: Explosives
Class 2: Gases
Class 3: Flammable liquids
Class 4: Flammable solids
Class 5: Oxidising substances & organic peroxides
Class 6: Toxic & infectious substances
Class 7: Radioactive material
Class 8: Corrosive substances
Class 9: Miscellaneous dangerous substances and articles, including environmentally hazardous substances that do not fall into classes 1-8.

The security requirements for carriage are split into two levels. There is a general level of requirements applicable to all dangerous goods and additional provisions for high consequence dangerous goods (HCDGs).

HCDGs are defined in RID & ADR Chapter 1.10.3.1.1 as those with the potential for misuse in a terrorist incident and which may, as a result, produce serious consequences such as mass casualties or mass destruction (whether to infrastructure, the environment or the economy) or, particularly for Class 7, mass socio-economic disruption. These levels apply to all modes of transport.

At the general level, all dangerous goods shall only be offered to carriers or organisations that have been appropriately identified. Temporary storage sites shall be properly secured, drivers and crew shall carry a means of photographic identification and security awareness training shall be provided. For HCDGs, a transport security plan is required to be adopted, implemented and complied with. Such a plan shall include: a review of operations, an assessment of security risks, a statement of measures to reduce those risks including training, procedures for dealing with breaches of security, and procedures for the evaluation and testing of plans. We would encourage you to use the security plan template in Annex 1 of this guidance.

The emphasis of the security work of the DfT is on the secure carriage of HCDGs to help ensure that industry is applying measures to reduce the risk of a serious incident. This is a combined guidance for the security of dangerous goods carriage by road and by rail (originally published in 2005 as two separate documents). The guidance is not intended to be prescriptive and organisations should consider the most appropriate way of complying with the requirements as applicable for their business.

Approach to Compliance

The purpose of the dangerous goods security regime is to reduce the vulnerability of dangerous goods being seized during transport on the road and/or rail network, or while at any temporary storage facilities, within Great Britain by terrorists and criminals for subsequent misuse e.g. in an attack on a crowded place or the transport system.

The scope of the regime covers: the goods loading area at the point of origin (e.g. the manufacturing site or airport/seaport), where the dangerous goods are stored waiting for loading, their carriage either by road or rail transport and intermediate temporary storage through to their delivery at the destination address.

DfT is focused on inspecting standards of security compliance at dangerous goods road and rail transport operations and follows a stepped approach to enforcement, similar to all other transport modes, with the emphasis on co-operation, advice, dialogue and self-rectification.

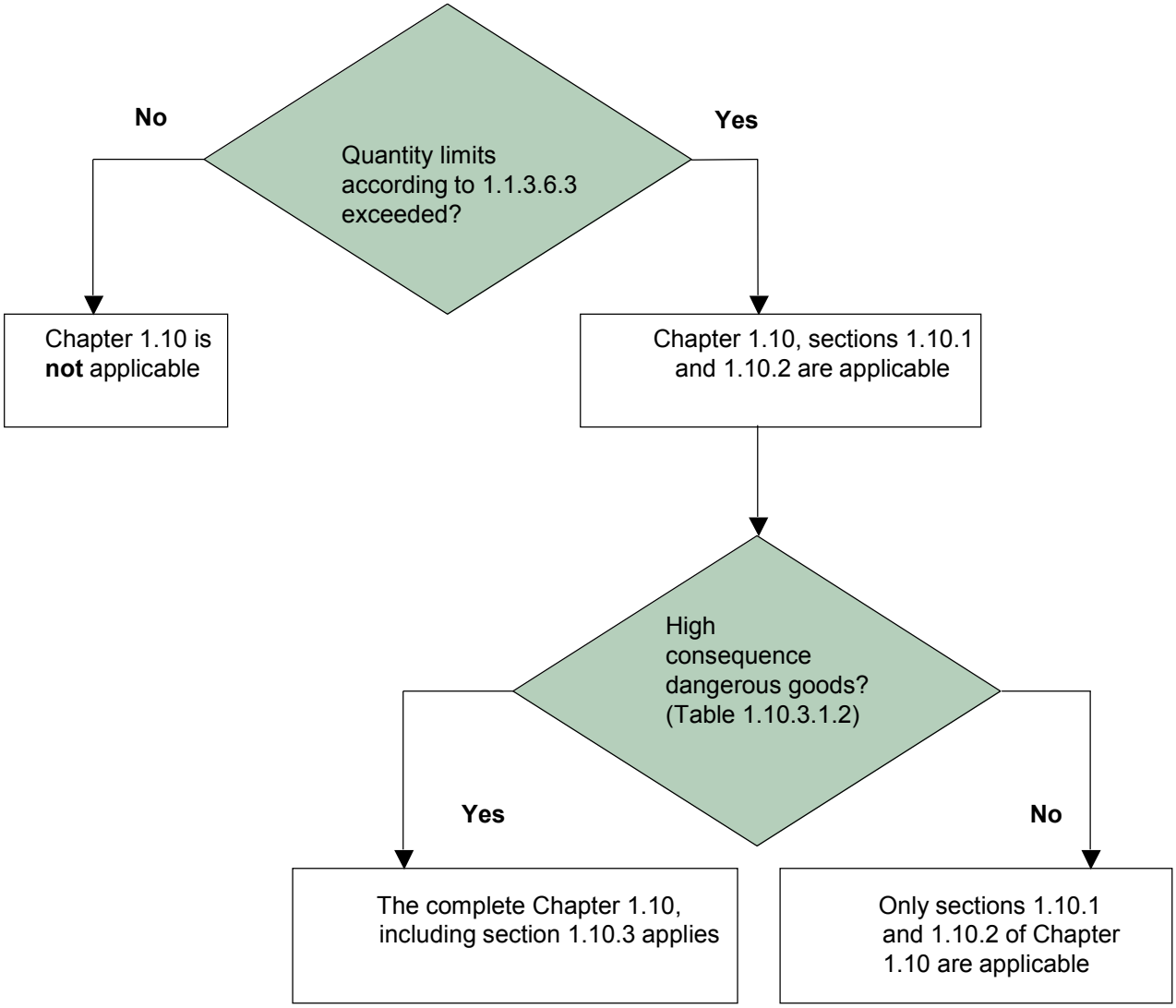
Compliance monitoring activities are conducted through a programme of announced inspections at operators or consignors premises to assess compliance with the mandatory aspects of Chapter 1.10 of RID and ADR. Prior to October 2012, this programme was delivered by the Vehicle and Operator Services Agency (VOSA, now Driver and Vehicle Standards Agency).

In 2014 DfT introduced covert security tests to this sector. These tests normally take place before or during compliance inspections and will usually be conducted having told a representative of the organisation. Feedback and lessons learned from the tests will be shared. Tests are typically of a short duration and are designed to test the effectiveness of an operator's information security or access control measures. Those involved in the carriage of HCDGs are required by the regulations to test their security plans, the tests conducted by the DfT inspectors are designed to help promote this practice and to improve security standards where appropriate. DfT inspection powers and the administrative and legal sanctions available derive from Section 19 of the Health and Safety at Work Act 1974 and Part III of the Railways Act 1993.

Dangerous Goods Security Enquiries

Enquiries regarding the security of dangerous goods can be made via email: DGSecurity@dft.gsi.gov.uk, or telephone: 020 7944 2881

Chapter 1.10 does not apply to the carriage of limited quantities and quantities below the levels set out in subsection 1.1.3.6.3 of ADR. It is important to note that in terms of security provisions, 1.1.3.6.3 also applies to tank and bulk transport by road vehicles. The following flow chart shows the decisions operators should take to establish how and to what extent Chapter 1.10 applies to their operation (quantity relates to packaged goods as well as to carriage in tanks and bulk containers):


Quantity limits according to 1.1.3.6.3 exceeded?
No
Yes
Chapter 1.10 is **not** applicable
Chapter 1.10, sections 1.10.1 and 1.10.2 are applicable
High consequence dangerous goods? (Table 1.10.3.1.2)
Yes
No
The complete Chapter 1.10, including section 1.10.3 applies
Only sections 1.10.1 and 1.10.2 of Chapter 1.10 are applicable

SECTION 2: COMPLYING WITH THE REGULATIONS

CHAPTER 1.10

SECURITY PROVISIONS

NOTE: *For the purposes of this Chapter, security means measures or precautions to be taken to minimise theft or misuse of dangerous goods that may endanger persons, property or the environment.*

1.10.1 General provisions

1.10.1.1 All persons engaged in the carriage of dangerous goods shall consider the security requirements set out in this Chapter commensurate with their responsibilities.

Advice

Any person engaged in the carriage of dangerous goods should consider the security requirements, be aware of the potential for their misuse, and follow the requirements of the regulations according to their level of responsibility. Depending on the size of the organisation, there could be one or more persons managing security. However, one person in an organisation should have overall responsibility and accountability for ensuring the security requirements are met.

Security should be included in the role of every person engaged in the carriage of dangerous goods, and to ensure that they understand their responsibilities it may be appropriate to include their responsibilities in job descriptions. These responsibilities and associated authority might include relatively simple requirements for security, such as identifying and reporting any person not authorised to be in a particular area or suspected of interfering with vehicles or wagons carrying dangerous goods. Managerial roles could include setting the security policy for a company, completing risk assessments and implementing security plans, ensuring application of security requirements at a transport business, storage facility, factory or terminal.

Rail operators and those with a direct connection to the rail network must have a Nominated Security Contact and Deputy with clearance to receive threat information and security notifications from DfT.

1.10.1.2 Dangerous goods shall only be offered for carriage to carriers that have been appropriately identified.

Advice

It is important that road and rail hauliers are appropriately identified. In the case of high consequence dangerous goods being carried, those companies are subject to regulation by the Land Transport Security Division within the Department for Transport for all hazard

classes except for class 7, which is regulated by the ONR. See page 6 for further information.

When offering goods to a road or rail transport contractor, written assurances should be obtained as part of a normal contractor or subcontractor approval process. They may be able to produce their most recent compliance report, for example, concerning compliance with the dangerous goods security requirements. As a minimum, when high consequence dangerous goods are being carried, it should be confirmed that the contractor holds a transport security plan.

Appropriately identifying carriers should also include checking drivers documents, including their photo ID and if applicable, their ADR vocational qualification. This could be done at their first visit to site, with on-going scheduled or random checks being carried out as part of a supplier audit. Dangerous goods should only be handed over to appropriately identified carriers whose driver can produce suitable identification.

Rail Freight Operating Companies hold a Safety Certificate issued by the ORR and this can form part of the appropriate identification process.

1.10.1.3 Areas within temporary storage terminals, temporary storage sites, vehicle depots, berthing areas and marshalling yards used for the temporary storage during carriage of dangerous goods shall be properly secured, well-lit and, where possible and appropriate, not accessible to the general public.

Advice

Temporary storage includes stops made necessary by the circumstances in a journey, as well as changes to the mode of transport. Areas used for the temporary storage of dangerous goods must be secured; this means they should be controlled by a combination of physical barriers, security equipment, procedures and staff vigilance.

Note: For the purposes of ADR & RID, parking or necessary short stops during a journey is not considered temporary storage.

To secure dangerous goods it is reasonable to consider a balance between staff presence and a secure perimeter fence to achieve the right outcome. All relevant areas should be subject to a security risk assessment to establish what measures are required to prevent unauthorised access, and action taken accordingly. It should be clearly identified in site plans which areas have restricted access. Visitors or contractors could be issued with temporary passes and escorted where appropriate; pass holders might only be given access to certain areas of the site in line with their duties and issued passes with photographic identification.

Restricting access to high consequence dangerous goods should be of higher concern and can be delivered in different ways.
A critical facility or building containing high consequence dangerous goods should have higher levels of security in place than other areas of the site.

Additional fencing or patrols could be considered around the areas where vehicles/trains are kept when loaded with high consequence dangerous goods.

Sensitive information, documents and IT should also be protected, see Annex 4.4.1. of this document for further guidance. It is important to consider the insider threat and transport information should be kept secure to ensure it is not released to unknown external parties.

Sites shall be well-lit where dangerous goods are kept. Illumination should complement other security equipment such as CCTV and enable any security patrols to be conducted effectively. Regular checks should be carried out to ensure that all security equipment and control measures are functioning correctly.

Rail carriers and companies which have connections to the rail network, such as refineries and terminal operators, will need to co-operate on security matters. Where appropriate, joint risk assessments should be conducted to ensure security of the rail network is adequately considered. There should be open discussions to ensure the security requirements can be met by all participants.

All reasonable steps should be taken to ensure unauthorised access to dangerous goods is prevented.

1.10.1.4 Each member of a vehicle crew shall carry with them means of identification, which includes their photograph, during carriage of dangerous goods.

Advice
Photographic identification must be carried at all times during carriage. In the case of train driver or crew member this could be the Safety Critical Card issued by the train operator, or Train Driving Licence. It may be appropriate for all staff working in terminals to be issued with photo ID passes. It is recommended that random spot checks of visiting drivers and crew member's photo ID passes are carried out. Staff should challenge persons on site who are not familiar and not wearing a pass.

1.10.1.5 Safety inspections in accordance with 1.8.1 and 7.5.1.1 shall cover appropriate security measures.

Advice
Please note that this requirement does not apply to rail operators (RID) as Section 1.8.1 relates to the administrative controls of the Competent Authority, so no advice is needed. However, in the ADR

regulations, and in accordance with section 7.5.1.1, drivers and vehicles are required to comply with security provisions and suitable vehicle inspections at sites where loading and/or unloading takes place. Sites receiving or despatching dangerous goods should have suitable measures in place for checking compliance before allowing entry to premises. This could include checking the driver's photographic identification & qualifications, and checking names & addresses on transport documentation.

1.10.1.6 The competent authority shall maintain up-to-date registers of all valid training certificates for drivers stipulated in 8.2.1 issued by it or by any recognized organization.

No advice is needed as this is the duty of the Competent Authority.

1.10.2 Security training

1.10.2.1 The training and the refresher training specified in Chapter 1.3 shall also include elements of security awareness. The security refresher training need not be linked to regulatory changes only.

Advice

All businesses and organisations are required to provide security awareness training for everyone engaged in the carriage of dangerous goods. A suitable training programme should be drafted and the subsequent training should be provided to all staff involved in dangerous goods transport operations. It should not be limited to drivers or production staff, but include anyone with security roles and responsibilities as well as anyone with access to transport information. The nature of the training can be tailored to suit the requirements of each organisation and relate to the staff member's level of responsibility. Goods vehicle and train crews play a key role in journey security, the vulnerabilities increase once the vehicle is on the road or rail networks. They should be provided with ongoing security awareness training and supplied with the latest available advice and guidance. More specific training should be given to those with specialised security duties or the management of security. DfT have produced a dangerous goods security training guidance document which can be accessed at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/318451/dangerous-goods-road-training.pdf

1.10.2.2 Security awareness training shall address the nature of security risks, recognising security risks, methods to address and reduce such risks and actions to be taken in the event of a security breach. It shall include awareness of security plans (if appropriate) commensurate with the responsibilities and duties of individuals and their part in implementing security plans.

Advice

The security awareness training must cover the topics listed above. DfT have produced a training film *'Lockdown'* to assist with delivering dangerous goods security training.

This can be used to supplement an operator's in-house training material and copies are available on request. Please send your requests to landsecurity@dft.gsi.gov.uk

Further security training can be obtained from private training suppliers or other government departments including the Centre for the Protection of National Infrastructure (CPNI) www.cpni.gov.uk and Counter Terrorism Security Advisers (CTSAs) www.gov.uk/government/organisations/national-counter-terrorism-security-office

The training should include awareness of the security plans when appropriate, what each person's role is in providing security and the company procedures to be followed for reporting suspicious activity, threats or breaches of security. A test of staff understanding and/or written advice could be provided on completion of the training.

1.10.2.3 Such training shall be provided or verified upon employment in a position involving dangerous goods transport and shall be periodically supplemented with refresher training.

Advice

The need to update staff on security issues should be reviewed every 2 years in light of the biennial revision of RID and ADR to ensure that the training that has been given remains current and correct. Refresher training should be provided at intervals of no more than 5 years, but the use of a greater frequency should be considered as part of the risk assessment process. The training programme should remind operators when refresher training is due and the records can be kept electronically or in hard copy.

New employees or contractors engaged in the carriage of dangerous goods must be provided with such training at the induction stages of their employment at the organisation or site. This should include what to do if the threat level changes. It is advisable to test the comprehension of the training and request they sign a document to confirm they have received and understood the training. The refresher training could be varied to suit changes in threat levels and any changes in the nature of any of the Operator's activities.

1.10.2.4 Records of all security training received shall be kept by the employer and made available to the employee or competent authority, upon request. Records shall be kept by the employer for a period of time established by the competent authority.

Advice

DfT have confirmed that training records must be retained in a secure location for a minimum of four years from the date of the training. Employees and DfT must be able to have sight of applicable training records on request.

1.10.3 Provisions for high consequence dangerous goods

1.10.3.1 ***Definition of high consequence dangerous goods***

1.10.3.1.1 High consequence dangerous goods are those which have the potential for misuse in a terrorist event and which may, as a result, produce serious consequences such as mass casualties, mass destruction or, particularly for Class 7, mass socio-economic disruption.

Advice

Transport operators involved in the carriage of dangerous goods should establish that there is a system where the consignor identifies to them any high consequence dangerous goods.

After initial set-up, such a system can then be applied to regular traffic. Whilst the gathering of information may follow the same system, it will be necessary to give specific consideration to determining and applying particular security requirements that may be necessary for an individual freight movement. A process will be needed to ensure necessary information is shared between the consignor, carrier and consignee.

1.10.3.1.2 High consequence dangerous goods in classes other than Class 7 are those listed in Table 1.10.3.1.2 below and carried in quantities greater than those indicated therein.

Advice

Duty holders should refer to this table, and those it references, to confirm if the dangerous goods are classified as high consequence.

Table 1.10.3.1.2: List of high consequence dangerous goods

Class	Division	Substance or article	Quantity		
			Tank (*l*) [c]	Bulk (kg) [d]	Packages (kg)
1	1.1	Explosives	[a]	[a]	0
	1.2	Explosives	[a]	[a]	0
	1.3	Compatibility group C explosives	[a]	[a]	0
	1.4	Explosives of UN Nos. 0104, 0237, 0255, 0267, 0289, 0361, 0365, 0366, 0440, 0441, 0455, 0456 and 0500	[a]	[a]	0
	1.5	Explosives	0	[a]	0
2		Flammable gases (classification codes including only the letter F)	3000	[a]	[b]
		Toxic gases (classification codes including letters T, TF, TC, TO, TFC or TOC) excluding aerosols	0	[a]	0
3		Flammable liquids of packing groups I and II	3000	[a]	[b]
		Desensitized explosives	0	[a]	0
4.1		Desensitized explosives	[a]	[a]	0
4.2		Packing group I substances	3000	[a]	[b]
4.3		Packing group I substances	3000	[a]	[b]
5.1		Oxidizing liquids of packing group I	3000	[a]	[b]
		Perchlorates, ammonium nitrate, ammonium nitrate fertilisers and ammonium nitrate emulsions or suspensions or gels	3000	3000	[b]
6.1		Toxic substances of packing group I	0	[a]	0
6.2		Infectious substances of Category A (UN Nos. 2814 and 2900, except for animal material)	[a]	0	0
8		Corrosive substances of packing group I	3000	[a]	[b]

[a] *Not relevant.*

[b] *The provisions of 1.10.3 do not apply, whatever the quantity is.*

[c] *A value indicated in this column is applicable only if carriage in tanks is authorized, in accordance with Chapter 3.2, Table A, column (10) or (12). For substances that are not authorized for carriage in tanks, the instruction in this column is not relevant.*

[d] *A value indicated in this column is applicable only if carriage in bulk is authorized, in accordance with Chapter 3.2, Table A, column (10) or (17). For substances that are not authorized for carriage in bulk, the instruction in this column is not relevant.*

1.10.3.2 ***Security plans***

1.10.3.2.1 Carriers, consignors and other participants specified in 1.4.2 and 1.4.3 engaged in the carriage of high consequence dangerous goods (see Table 1.10.3.1.2) or high consequence radioactive material (see 1.10.3.1.3) shall adopt, implement and comply with a security plan that addresses at least the elements specified in 1.10.3.2.2.

Advice

The security plan(s) should be based on the overall operation of the business, not on individual movements, and tailored to suit the company's operational activities. The drafting and format of the security plan(s) should take into account the business operation in deciding how to structure the plan(s); each organisation should decide which approach suits them best. It should be noted that the requirements listed at 1.10.3.2.2 (a) to (h) are the minimum for inclusion.

It may be more appropriate to implement a security plan for each site or location which is used during the carriage of high consequence dangerous goods, as there may be many different characteristics and security measures at each. It may be more appropriate for some operators to implement a company-wide security plan rather than on a site by site basis. It is strongly advised that operators work with the sites consigning or receiving high consequence dangerous goods to ensure security has been adequately assessed and security plan(s) are in place for all participants as required.

Plan(s) should take into account other plans which may be in place, such as Maritime Security Plans or Emergency Plans, as well as any risk to the site or carrier and any unique circumstances or location of premises. Security plan(s) should be considered 'live' documents and kept under review so that they reflect changes in: products handled, sites, the nature of the operation and key personnel. Security plans and procedures should be tested by holding regular exercises that adequately test security measures, such as an access control test.

The plan(s) should clearly identify those involved in the dangerous goods transport chain and what their security roles and responsibilities are, including dealing with security incidents.

1.10.3.2.2 The security plan shall comprise at least the following elements:

(a) Specific allocation of responsibilities for security to competent and qualified persons with appropriate authority to carry out their responsibilities;

Advice

The appropriate person or persons with responsibility for the management of security will depend upon the size of the business. If there are several sites within the business, it may be prudent to

appoint one person with overall responsibility and authority for implementation of security and perhaps have a security coordinator or manager at each site.

The same person should control the security plan and share the information as required within the organisation. Security responsibilities should be documented in the security plan and should form part of job role specification, or might be included in a person's job description.

(b) Records of dangerous goods or types of dangerous goods concerned;

Advice
A summary of the types of dangerous goods regularly carried or potentially carried should be included, this could be a table which identifies just the UN classes. If practical, the UN numbers and shipping names could be listed, identifying which are HCDG.

A reference to the Dangerous Goods Safety Adviser (DGSA) annual report could be made which should include a summary of the dangerous goods moved over the previous twelve months. Records of dangerous goods should be kept for a minimum of three months from the date of carriage.

(c) Review of current operations and assessment of security risks, including any stops necessary to the transport operation, the keeping of dangerous goods in the vehicle, tank or container before, during and after the journey and the intermediate temporary storage of dangerous goods during the course of intermodal transfer or transhipment between units as appropriate;

Advice
An overview of the current operation should be included at the start of the security plan to describe its purpose and scope. This will set out the reasons for the plan, how and why it applies to the business and to the carriage of high consequence dangerous goods. A regular review will be required to determine any changes to security procedures or arrangements that might be necessary.

A key objective is to reduce the potential risk as far as possible by expediting the carriage and specifically minimising or eliminating the time high consequence dangerous goods are stopped on route. For example, eliminating overnight stops or breaks in the journey and minimising the time between delivery and collection are aspects that could be considered.

(d) Clear statement of measures that are to be taken to reduce security risks, commensurate with the responsibilities and duties of the participant, including:

- training;
- security policies (e.g. response to higher threat conditions, new employee/employment verification, etc.);
- operating practices (e.g. choice/use of routes where known, access to dangerous goods in intermediate temporary storage (as defined in (c)), proximity to vulnerable infrastructure etc.);
- equipment and resources that are to be used to reduce security risks;

Advice
The security plan must include these measures which help contribute to transport security. The specific instructions and guidance given to drivers and crew plus what specific measures are taken in the event of unplanned or unusual circumstances should be included in this section.

Training
See section 1.10.2 of this guidance.

Security Policies
Advice
A security policy statement should be written and included in the plan(s). Depending on the nature of the operation, and potential vulnerabilities, there should be documented predetermined arrangements to respond to changes in the National or Modal threat levels.

The security plan should consider changes to business or national threat levels. Up to date information and guidance regarding the National Threat Levels can be accessed via the following link https://www.mi5.gov.uk/home/the-threats/terrorism/threat-levels.html

Employment Checks
Advice
Suitable checks should be made on any potential new employees who will be involved with the transport of high consequence dangerous goods. The verification of original identity documents, licences or qualifications and permission to work in the UK is necessary. Five year employment record checks should be made on everyone engaged in the transport of high consequence dangerous goods. The type of checks you should carry out are likely to be part of a routine recruitment process. However, it may be necessary for Rail Freight Operating Companies to carry out additional or higher level security checks on staff who will be DfT Nominated Security Contacts.

Operating practices

Advice

The plan should document how high consequence dangerous goods are accepted and the process for determining specific security requirements necessary for a particular movement such as:

- how movements are controlled and monitored to ensure security;
- how any problems with the movement are dealt with, for example security during unplanned stoppages;
- how road and rail interfaces are managed at intermodal depots; and
- how public access to vehicles or trains has been restricted.

Equipment and resources

Advice

The security plan statement of measures must also identify and record the equipment and resources deployed in the security arrangements for high consequence dangerous goods movements. It is possible that the equipment may not be solely for that purpose, e.g. lighting may be provided for operational safety and CCTV in place for preventing vandalism and criminal activity. This section should also identify what resources are available and utilised when there are necessary breaks in a journey.

(e) Effective and up to date procedures for reporting and dealing with security threats, breaches of security or security incidents;

Advice

If there is a security incident or a security concern, there must be a system or procedure in place for reporting such occurrences. There should be an internal procedure to guide staff on what action to take and who they should report to. Information should be shared or exchanged with other carriers, consignors, competent authorities as well as Police or Security Services, dependent on the nature of the incident. This process should be recorded in the security plan.

(f) Procedures for the evaluation and testing of security plans and procedures for periodic review and update of the plans;

Advice

The requirement for testing of security plans could be integrated into existing quality and management systems. Testing procedures could be extended to include access control or staff vigilance tests at locations where high consequence dangerous goods are stored during transport. Testing of the security plan could also take place in the form of desktop exercises or any other test which adequately tests the security measures in place.

As well as keeping a record of the tests, and investigating any 'failures', it is good practice to review and, if necessary, update the security plan on a regular basis, preferably annually, to ensure the accuracy of its content and to consider updating the security plan following any security incident or test where lessons have been learned.

(g) Measures to ensure the physical security of transport information contained in the security plan; and

Advice
The security plan must be protected from unauthorised access e.g. held electronically on a password-protected computer in a location with restricted access. If printed, the plan should be kept secure and treated as a sensitive document, only shared with emergency services or control authorities on request. Everyone with access should be aware the information it contains should only be made available on a need to know basis.

(h) Measures to ensure that the distribution of information relating to the transport operation contained in the security plan is limited to those who need to have it. Such measures shall not preclude the provision of information required elsewhere in ADR or RID.

Advice
The security plan should advise how the distribution of information about the dangerous goods transport operations is restricted to only those who need the information.

NOTE: *Carriers, consignors and consignees should co-operate with each other and with competent authorities to exchange threat information, apply appropriate security measures and respond to security incidents.*

Advice
The above note is for all participants engaged in the carriage of high consequence dangerous goods by road and rail. It also includes all bodies with access to the rail network including BTP, Network Rail and DfT. There should be an internal reporting procedure in place to record any security related incidents, which once investigated, could be shared internally to all sites and cascaded externally through membership of trade organisations, or by attendance at industry forums. The need to co-operate also extends to determining and documenting processes and arrangements to exchange information and apply appropriate security.

1.10.3.3 Devices, equipment or arrangements to prevent the theft of the vehicle carrying high consequence dangerous goods (see Table 1.10.3.1.2) or high consequence radioactive material (see 1.10.3.1.3) and its cargo, shall be applied and measures taken to ensure that these are operational and effective at all times. The application of these protective measures shall not jeopardize emergency response.

Advice

The application of measures to prevent theft will need to be determined by the transport operator with input from the consignors. Examples of devices and equipment includes locks, seals and tracking devices. Specialist advice should be sought from commercial organisations, DfT, BTP, CTSAs or CPNI when appropriate. There should be a system in place for reporting failures of devices, equipment or arrangements. It is advisable that drivers have an emergency means of communication at all times when carrying high consequence dangerous goods.

Arrangements covers the operational procedures that are in place, which might include the deployment of resources to provide surveillance, placing of shipping containers door to door to prevent access, or ensuring specific measures are in place for particularly sensitive goods such as operating non-stop services.

NOTE: *When appropriate and already fitted, the use of transport telemetry or other tracking methods or devices should be used to monitor the movement of high consequence dangerous goods (see Table 1.10.3.1.2) or high consequence radioactive material (see 1.10.3.1.3).*

Advice

Total Operations Processing System (TOPS) and Global Positioning System (GPS) applications are in use on some trains. Tracking systems are widely available for goods vehicles and trailers; fitting such equipment represents best practice when carrying high consequence dangerous goods. It may also be appropriate to consider tracking the freight or container itself if the goods are particularly sensitive or attractive to thieves.

1.10.4 In accordance with the provisions of 1.1.3.6, the requirements of 1.10.1, 1.10.2, 1.10.3 and 8.1.2.1 (d) do not apply when the quantities carried in packages on a transport unit do not exceed those referred to in 1.1.3.6.3, except for UN Nos. 0029, 0030, 0059, 0065, 0073, 0104, 0237, 0255, 0267, 0288, 0289, 0290, 0360, 0361, 0364, 0365, 0366, 0439, 0440, 0441, 0455, 0456 and 0500 and except for UN Nos. 2910 and 2911 if the activity level exceeds the A_2 value (see first indent of 1.1.3.6.2). In addition, the requirements of 1.10.1, 1.10.2, 1.10.3 and 8.1.2.1 (d) do not apply when the quantities carried in tanks or in bulk on a transport unit do not exceed those referred to in 1.1.3.6.3. In addition the provisions of this Chapter do not apply to the carriage of UN No. 2912 RADIOACTIVE MATERIAL, LOW SPECIFIC ACTIVITY (LSA-I) and UN No. 2913 RADIOACTIVE MATERIAL, SURFACE CONTAMINATED OBJECTS (SCO-I).

Advice

This relates to limited quantities referenced in ADR & RID, below which the requirements of these security provisions do not apply.

ANNEX 1 SECURITY PLAN TEMPLATE

[INSERT FULL BUSINESS NAME]

ROAD / RAIL TRANSPORT SECURITY PLAN

RESTRICTED

[When completed]

IMPLEMENTED

[Insert date]

Guide to completing a security plan [Delete this page once completed]

For those engaged in the carriage of high consequence dangerous goods, the implementation of a transport security plan is a mandatory requirement as detailed in Chapter 1.10 of the ADR & RID Regulations.

High consequence dangerous goods are defined in the regulations as those which have the potential for misuse in a terrorist event and which may, as a result, produce serious consequences such as mass casualties, mass destruction or, particularly for Class 7, mass socio-economic disruption.

The list of high consequence dangerous goods can be found at sub chapter 1.10.3.1.2. The provisions of chapter 1.10 do not apply to the carriage of limited quantities and quantities below the levels of subsection 1.1.3.6.3 of ADR. It is important to note that in terms of security provisions, 1.1.3.6.3 also applies to tank and bulk transport by road vehicles.

Delete or mark as N/A any parts of this template that are not applicable to you. Add any further transport or site related security information not included within this template. This is only a suggested template, you could choose to adopt this, adapt this, or create one of your own that suits your operation.

If you have a road and rail connection, you may choose to create a combined document for both operations; it is also acceptable to keep them separate. For operators with multiple sites, you may wish to create one company-wide security plan for the whole operation, or one for each transport site. Do what is best for your operation.

The completed plan must address at least all the elements specified in sub chapter 1.10.3.2.2 of the ADR & RID regulations.

For further advice please refer to the Dangerous Goods security guidance which can be found at: https://www.gov.uk/government/publications/security-requirements-for-moving-dangerous-goods-by-road-and-rail

CONTENTS PAGE

SECTION 1: Business details

1. Name of company/organisation

[Insert text]

2. Full correspondence address

[Insert text]

3. General telephone and e-mail contact details

[Insert text]

4. Full address(es) of location(s) security plan applies to

[Insert text]

5. Telephone and e-mail contact details for site security plan applies to

[Insert text]

6. Name of nominated security co-ordinator

[Insert text]

7. Contact details for this security co-ordinator

[Insert text]

8. Training given to security co-ordinator

[Insert text]

9. Name of the Dangerous Goods Safety Advisor (DGSA)

[Insert text]

10. Overview of current operations.

[Insert text. This section should contain a description of the business, provide an overview of the current transport operations and the function of sites it applies to. It should explain the purpose and scope of the security plan and why it is in place.]

11. List of dangerous goods

[Insert text Classes carried if long list of UN numbers, indicate which are HCDG]

SECTION 2: Management of security

(1) PEOPLE

Who is ultimately responsible for the management and control of the security plan?

[Insert text]

Procedures for recording meetings and actions with regard to security

[Insert text]

Procedures for receiving and disseminating security information to relevant staff

[Insert text]

List of other people responsible for the management of security issues that the security plan applies to, and their duties

See Annex A

List of people authorised to handle high consequence dangerous goods

See Annex B

Risk assessment of current transport operations

See Annex C [if the risk assessment is too detailed to be included in the security plan, then state where the document is stored]

Details of people who have access to the security plan

See Annex D

Record of reviewing and updating the security plan.

See Annex E

Site Plans showing the location of all restricted areas, controlled buildings, protected areas and access points to these areas and buildings, company and visitor parking.

See Annex F

(2) RESPONSE TO AND REPORTING OF SECURITY THREATS, INCIDENTS, AND BREACHES OF SECURITY

Reporting procedures

[Insert text]

Recording procedures

[Insert text]

Security incident investigation procedure

[Insert text]

(3) EVACUATION PROCEDURES AND ROUTES

Details of evacuation procedures

[Insert text]

Details of muster points and safe refuge areas

[Insert text]

(4) SECURITY OF INFORMATION

Security procedures for hard copy information considered security sensitive

[Insert text]

Security procedures for electronic information considered security sensitive

[Insert text]

How will the records of dangerous goods movements be kept?

[Insert text]

(5) SECURITY EQUIPMENT

Details of site security equipment

[Insert text]

Details of maintenance programme for security equipment

[Insert text]

Action to be taken if equipment fails

[Insert text]

Details of vehicle security equipment

[Insert text]

Action to be taken if equipment fails

[Insert text]

(6) SECURITY TRAINING

Details of dangerous goods security awareness training programme for all staff

[Insert text]

Details of security refresher training

[Insert text]

Details of training programme for personnel with specific security duties

[Insert text]

Details of procedures for maintaining training records (Where they are kept, how long for and who has access to them)

[Insert text]

(7) SECURITY TESTS

Details of security drills and testing of the security plan

[Insert text]

(8) DETAILS OF HOW CONSIGNORS, CARRIERS AND/OR DRIVERS WILL BE APPROPRIATELY IDENTIFIED

[Insert text]

(9) DETAILS OF NEW EMPLOYEE VERIFICATION PROCESS

[Insert text]

SECTION 3: Communication

(1) COMMUNICATION LINKS

Details of communication links with drivers

[Insert text]

Details of any back-up communication links

[Insert text]

Details of vehicle monitoring or tracking

[Insert text]

(2) SECURITY ALERTS

People to be informed of a site security alert

[Insert text]

People to be informed of a journey security alert

[Insert text]

Action to be taken following a security alert

[Insert text]

(3) COOPERATION WITH OTHER PARTIES

Details of how threat information is exchanged with carriers, consignors, consignees and competent authorities

[Insert text]

Details of how security information is shared with carriers, consignors, consignees, infrastructure managers and competent authorities

[Insert text]

Response to changes in national threat conditions

[Insert text]

(4) RESPONSE AGENCIES

Department for Transport
Land Transport Security Division
Great Minster House
33 Horseferry Road
London
SW1P 4DR
Tel: 020 7944 3288
E-mail: landsecurity@dft.gsi.gov.uk

Police [Insert name of Police Service or CTSA]

Contact name:	[insert text]
Address:	[insert text]
Telephone number:	[insert text]
24hr telephone number:	[insert text]
Fax:	[insert text]
E-mail:	[insert text]

MoD (If applicable)

Contact name:	[insert text]
Address:	[insert text]
Telephone number:	[insert text]
24hr telephone number:	[insert text]
Fax:	[insert text]
E-mail:	[insert text]

DVSA (If applicable)

Contact name:	[insert text]
Address:	[insert text]
Telephone number:	[insert text]
24hr telephone number:	[insert text]
Fax:	[insert text]
E-mail:	[insert text]

Other

Name of authority:	[insert text]
Contact name:	[insert text]
Address:	[insert text]
Telephone number:	[insert text]
24hr telephone number:	[insert text]
Fax:	[insert text]
E-mail:	[insert text]

SECTION 4: Measures of site security

(1) DESIGNATED PROTECTED AREAS, BUILDINGS AND LOCATIONS WHERE DANGEROUS GOODS ARE TEMORARILY STORED IN THE COURSE OF TRANSPORT

List of restricted areas and buildings, indicate if members of the public are allowed access.

Area 1 [insert text]
Area 2 [insert text]
Area 3 [insert text]
Area 4 [insert text]
Area 5 [insert text]

Building 1 [insert text]
Building 2 [insert text]
Building 3 [insert text]
Building 4 [insert text]
Building 5 [insert text]

Details of people responsible for checking & controlling access to these areas.

[Insert text]

(2) SECURING RESTRICTED AREAS FROM UNAUTHORISED ACCESS

Details of equipment such as fencing, walls, gates or any other features used to protect restricted areas or buildings from unauthorised access

[Insert text]

Details of procedures in place for preventing unauthorised access to dangerous goods

[Insert text]

Measures in place to restrict access at control points

[Insert text]

Procedures for dealing with unauthorised access

[Insert text]

(3) PASS SYSTEMS

Details of pass system in operation

[Insert text]

Details of pass system record keeping

[Insert text]

Action to be taken when pass is lost

[Insert text]

Procedures for retrieving passes when no longer used and for revoking passes

[Insert text]

Procedures for auditing system of passes

[Insert text]

(4) MONITORING RESTRICTED AREAS, CONTROLLED BUILDINGS AND AREAS TO PROTECT

Lighting

[Insert Details of security lighting in place]

Details of CCTV systems and procedures

[Insert text, list of places monitored using CCTV]

Details of recording equipment and procedures

[Insert text]

Details of Perimeter Intrusion Detection systems in place

[Insert text]

Details of procedures for recording and responding to alarms

[Insert text]

(5) SECURITY PATROLS (where applicable)

Details of how security patrols will be conducted

[Insert text]

Procedures for responding to security incidents

[Insert text]

Procedures for reporting security incidents

[Insert text]

Journey security procedures, including stops, routing & parking

[Insert text]

(6) VEHICLE/TRAIN/WAGON PROTECTION

Details of equipment fitted to goods vehicles, trains & wagons, or of procedures in place to prevent theft or interference when carrying dangerous goods

[Insert text]

Any miscellaneous information

Use this section to provide any additional information you feel is relevant to transport security.

Security Plan Annex A: List of people responsible for the management of security issues and their duties

NAME	POSITION	DUTIES

Security Plan Annex B: List of people authorised to handle high consequence dangerous goods

This may not be practicable for large companies

Security Plan Annex C: Risk assessment of current operations

Security Plan Annex D: List of people who have access to the security plan

Security Plan Annex E: Record of when the security plan has been reviewed or amended

REVIEW OR AMENDMENT DATE	AMENDMENT MADE

Annex F: Site Plan (Site plan should indicate restricted areas)

ANNEX 2: SECURITY ADVICE - SITE & DEPOT

2.0 Assets

2.01 This section highlights effective measures to improve the physical security at storage sites including depots, and on vehicles used for the transport of high consequence dangerous goods.

2.02 Physical security is designed to make it as difficult as reasonably practical for any intruder to steal dangerous goods. Detection and prevention of theft of the goods by your own staff should be built into your organisation's procedures.

2.03 Good security is a combination of physical measures, sound procedures and the awareness and attitude of managers and employees. Actual measures may vary from site to site, depending on the nature of the business.

2.04 All good physical security regimes are based on the 3D principle – deter, detect and delay.

2.05 **Deter** – the overt physical and electronic security measures that might deter a would-be intruder.

2.06 **Detect** – alarm systems, with visual (CCTV) verification, to detect the presence of an intruder.

2.07 **Delay** – physical security measures that delay the intruder long enough to hopefully allow a response force to attend.

2.08 But if the 3D principle is to work, detection must come before delay.

2.09 Vehicle operators are not expected to be responsible for the security of overnight parking or stops on route such as service stations. However, you should consider these areas in your security plan (if applicable).

2.1 Sites

2.1.1 Thefts from premises remain one of the largest problems for operators. Thieves can often work out that vehicles and their loads will be on the premises at regular times.

2.1.2 There are a number of ways to improve vehicle and premises security. Effective depot security will buy time, a vital factor in crime prevention. However, effective security is not always cheap, so it is important to assess your needs carefully.

2.1.3 Security measures may vary depending on the type and quantities of dangerous goods your organisation handles, and how often. This section sets out some guidance on what to consider at the various types of sites and operations.

2.1.4 Site security should be addressed where vehicles or goods are temporarily stored. i.e. ready for shipment or in transit. The security requirements will not cover owners of overnight parking facilities. Operators should try to park their vehicles in a secure

place and in accordance with ADR Chapters 8.4 and 8.5, concerning the supervision of vehicles.

2.1.5 Many sites will incorporate perimeter security fencing to meet Health & Safety requirements, as well as security requirements. However, this guidance recognises that perimeter fencing might not be applicable in all cases. It is important to remember that the implementation of security measures should be pragmatic, proportionate and sustainable.

2.1.1 Nature of Operation

There are four broad levels of sites.

2.1.1.1 **Level 1** – non-high consequence dangerous goods are held, the quantities are small or they are handled infrequently.

2.1.1.2 **Level 2** – non-high consequence dangerous goods are held but in larger quantities and/or on a more frequent basis.

2.1.1.3 **Level 3** – small quantities of high consequence dangerous goods are held.

2.1.1.4 **Level 4** – large quantities of high consequence dangerous goods are held.

2.1.1.5 Some classes of high consequence dangerous goods may need to be included in Level 4 even though they are only being stored in small quantities, such as pathogens & toxins.

2.1.1.6 Measures identified later in the guidance document will build upon these basic levels of security. You should focus your resources on the highest risk first.

Level 1

2.1.1.7 Secure those parts of the site where you store dangerous goods, consider all applicable legislation when deciding on site security specification. A safe may be big enough to store small quantities of dangerous goods securely. For slightly larger quantities it might be sufficient to install a secure cage, constructed of weld-mesh material with a locking door, possibly to British Standards such as BS1722:2006 Part 10 (fencing) and BS3621:2007 (locks), subject to any other regulatory requirements. Limit access to secure storage areas to appropriately recruited and trained staff.

Level 2

2.1.1.8 Level 2 sites are where the quantities of dangerous goods held are large enough to warrant larger areas of the site being secured or even the whole site. If dangerous goods are stored openly on site, then you could use weld mesh or palisade fencing; when replacing or building a new fence it is recommended that it is constructed to BS1722:2006 Part 10 or Part 12. You could also control access via a pass system. If you store dangerous goods in vehicles or secure buildings, then fencing may be chain link so long as vehicles are adequately secured. There may be occasions when fencing or access control may not be required, consider all other applicable

regulations before deciding.

For example fences may not be required if:

- vehicles have high quality security;
- trailers cannot be detached or towed away; or
- there are bollards to prevent vehicle access/egress.

Level 3

2.1.1.9 At sites where small quantities of high consequence dangerous goods are stored, as with level 1, localised storage may be appropriate, or perhaps 'double layered' security such as a safe within a cage.

Level 4

2.1.1.10 Perimeter security of level 4 sites should comprise of good quality weld mesh or palisade fencing, preferably constructed to BS1722:2006 Part 10 or 12 standard. Access should ideally be controlled with photographic identification.

2.1.1.11 Security fencing is best fitted with intruder detection equipment that alerts a security control point (possibly the Police).

2.1.1.12 There is no requirement for Perimeter Intruder Detection Systems (PIDS) in the regulations, but on opening of the site each day you should check the secure storage and if anything has been stolen or there are signs of interference or attempted theft, this should be reported to the Police, Home Office or other appropriate authorities/other legislative requirements as appropriate.

2.1.1.13 Sites that store dangerous goods classified under the Control of Major Accident Hazards (COMAH) regulations are likely to have aspects of security considered, including personnel. However, you cannot take this for granted. In particular, site location may be a factor. If you think you need it you can obtain security advice from your local CTSA, their contact details can be found at:

https://www.gov.uk/government/publications/counter-terrorism-support-for-businesses-and-communities

2.1.1.14 Improved security measures may give rise to location and design concerns, particularly in relation to any sites located in areas of designated value, such as conservation areas. In some cases, local planning authorities may be disposed to conclude that planning permission ought to be refused because of such concerns. Guidance has been issued to local planning authorities on how to strike a balance between local amenity requirements and providing appropriate levels of security.

2.1.2 Security risk assessments

2.1.2.1 Assessing the risks you face, categorising them, and then deploying appropriate measures to reduce them is an important part of improving site security. The four levels of sites described above are useful as a guideline in determining the nature of your operation. However, a risk assessment will help you identify what security

measures to consider within a chosen level.

2.1.2.2 A risk in the context of security is a measure of the probability that an unlawful act will be attempted and will be successful. The level of risk is affected by a combination of the threat your operation faces and the vulnerability of the target.

2.1.2.3 A risk assessment will give you an estimate of the probability that an unlawful act will be attempted and will succeed.

2.1.2.4 The CPNI have produced the Guide to Producing Operational Requirements for security measures which outlines all of the information you need to assess risk and produce a statement of your overall security needs. Level 2 of the guide contains an assessment of the detailed security needs such as fences and gates. The guide can be found at:

http://www.cpni.gov.uk/documents/publications/2010/2010-word_op_reqs.doc?epslanguage=en-gb

2.1.2.5 We recommend that you produce a written statement of your overall security needs as described in level 1 of the guide, even if you are a small business handling only a small amount of dangerous goods. Going through the process will help you be clear about what your risks are and will be evidence that you have actually considered security and its implications. The process does not need to be time consuming or be over complicated as you are already aware of your business and operational environment.

2.1.2.6 This guidance contains a security risk assessment template at Annex 6. This template is only a guide but once completed can be the basis of your written statement. Your organisation's own risk assessment design could also be used for consistency.

2.1.3 Securing premises

2.1.3.1 Police and your insurer may be able to give advice on securing premises using such measures as:

- perimeter protection (fences);
- site access and control (barriers);
- surveillance (illumination and CCTV);
- guards;
- intruder detection;
- visitor control;
- limiting the number of key holders;
- staff parking away from the main site;
- controlled access to loading bays, vehicle key storage and control systems;
- personnel and vehicle search procedures; and
- security of any tools or equipment that might help criminals to steal vehicles or loads.

2.1.3.2 The right perimeter illumination should make it easier to identify intruders and vehicles. CCTV surveillance systems should be able to monitor, detect, recognise or

identify. They should be linked with other perimeter intruder detection systems and physical delay measures. In some circumstances, lighting may not be appropriate, in which case other methods of illumination, such as infra-red may be suitable. Regulations require adequate lighting to be in place at areas where dangerous goods are stored temporarily during the course of transport.

2.1.3.3 The aforementioned Guide to Producing Operational Requirements contains detailed guidance on how to assess your needs for and installing the following:

- perimeter fencing;
- security lighting;
- CCTV;
- perimeter intruder detection systems;
- physical delay measures; and
- intruder detection systems.

2.1.4 Restricting access

2.1.4.1 Visits to sites should be scheduled and security personnel should be told of the visit beforehand. Visitors should be accompanied throughout their visit and are the responsibility of the host, who should be a member of staff.

2.1.4.2 Many sites already require visitors to deposit all electronic equipment at the gatehouse before entering. Consider extending this practice on security grounds.

2.1.4.3 Employers can reduce the ‘insider’ risk by limiting an individual employee's access to key locations, assets and information to that which they need to do their job. This can be done in various ways, depending on the nature of the business.

2.1.4.4 Examples include:

- physically controlling access to locations housing critical plant, high consequence dangerous goods, IT systems or expensive assets;
- protecting business-sensitive information, whether in hard copy (by, for example, locking it up securely) or soft copy (using access controls on IT systems);
- requiring staff to wear photo ID passes at all times;
- controlling or limiting unsupervised access by contract/agency staff.

2.1.5 Access control

2.1.5.1 Site operators should determine whether and how to control access. Ensure that areas used for the temporary storage of dangerous goods during carriage are properly secure and where possible not accessible to the general public. When securing entry points, consider emergency exits and disabled access.

2.1.5.2 You also need to establish minimum security requirements, which will potentially prevent tailgating and the possibility of bypassing barriers.

2.1.5.3 Unexpected vehicles should be refused entry to a site until their identity and proof of need for entry has been confirmed.

2.1.6 Searching on entry and exit

2.1.6.1 Some companies have a policy of 'on-the-spot' vehicle and body searches as part of their theft prevention strategy. Where appropriate, it should be a condition of entry and/or exit to a site that people may undergo a body search. This is particularly important at sites that are involved with pathogens, toxins, munitions or explosives.

2.1.6.2 Body searches should be witnessed and only trained staff should carry them out. If you feel you need such search procedures, include compliance with them in employees' terms and conditions.

2.1.6.3 Where there are areas of particular sensitivity and/or risk, employers may also want to consider random searching on entry and exit.

2.1.7 Storage of vehicles

2.1.7.1 Overnight storage of vehicles in locked buildings is often only practical for light vans. Heavy commercial vehicles need more space, and are generally kept outside. Where vehicles are stored inside, consider the fire risk.

2.1.7.2 Avoid leaving vehicles against fences in the belief that they will be secure. Although the fence may protect the rear doors from being opened, the top and sides remain vulnerable. Backing vehicles up against each other provides only limited security to the rear doors. Wherever possible, park vehicles close together with loaded vehicles towards the centre.

2.1.7.3 If high consequence dangerous goods are pre-loaded for departure, they are of course more vulnerable if left overnight. Wherever practicable, vehicles should not be left loaded overnight or for any significant period of time before departure. If vehicles have to be pre-loaded for operational reasons, leave them in a secure location, locked, with any alarms or immobilisers set and the keys kept in a safe place. Consider removing any key identity tags with vehicle numbers on. Also, inform the local guard force or security monitoring firm where applicable.

2.1.8 Fencing

2.1.8.1 Perimeter fencing is important as it creates the first physical barrier to a site. When considering what type and size of fencing to install, bear in mind local planning authority concerns with regard to the impact on the surrounding environment.

2.1.8.2 There are several British Standard and commercial fences in common use for site security. But even the most secure types can eventually be scaled, penetrated or burrowed under by a well-prepared intruder who is strong, agile and determined.

2.1.8.3 The most commonly used fence is the relatively inexpensive chain link fence. However, it is only capable of delaying a reasonably agile intruder for a very short time.

2.1.8.4 The welded mesh version of BS1722:2006 Part 10 or the security pattern (SP) steel security palisade fences to BS1722:2006 Part 12 have very useful characteristics.

The latter is strong and rigid and offers excellent opportunities for mounting some type of PIDS and improves intruder delay time.

2.1.8.5 However, if a perimeter is next to a public road, footpath or other frequented area, a single fence mounted with a PIDS may signal an alarm so frequently as to be useless; consider alternative outdoor detection for perimeter surveillance. Where a higher level of perimeter security is required, the answer may be a double fence, with the inner fence alarmed, or with an alarmed strip between the two fences. The innermost fence should be the hardest to scale and penetrate to ensure the greatest delay.

2.1.8.6 At sites with long perimeters, a strong perimeter fence may not be practicable. In such cases, it may be better to concentrate on the areas that need the highest level of protection.

2.1.8.7 Some operators have installed electric or electrified fences, which can provide both an alarm system and a powerful deterrent.

2.1.8.8 Remember that criminals will always try to find a way into secure areas. You cannot rely on rivers and fields to provide a secure natural boundary.

2.1.8.9 Many fences such as BS1722:2006 Part 10 include strands of barbed wire. Some have barbed wire coils (or concertinas) on top while a few incorporate barbed tape.

2.1.8.10 Barbed wire, whether in coil or strand form, is much less effective as a deterrent and as a practical defensive measure than the various barbed tapes. However, to avoid legal problems, you should only place barbed tape where it is well out of the reach of passers-by. Furthermore, if you place it on top of a fence to discourage scaling, it must be out of reach of children. This tends to limit its use to fences that cannot be climbed without scaling equipment. Again, to avoid legal problems, you must make it obvious to the public that barbed wire or tape is in use.

2.1.8.11 You should ensure that fences are fitted in accordance with the relevant British Standard and that you set up a maintenance programme.

2.1.9 Gates

2.1.9.1 Fit gates that are appropriate to the risk. Gates must be compatible with and at least as strong as the perimeter fence. The best, and most expensive, are electric sliding gates that run in ‘tramways’ rather than those suspended from hinges, as these are far more robust. They will require pedestrian access if not manned 24 hours. An alternative is a good set of metal gates with effective locks.

2.1.9.2 Other effective measures include gates capable of being double-locked with the hinges welded to prevent them being lifted off. Tap or weld screws wherever possible to prevent their removal. The same applies to the screws and hinges on vehicle locks.

2.1.9.3 Use a good security padlock of hardened steel. Make sure the bar on any standard padlock you use is as short as possible and shroud the padlock with hardened steel.

This makes it harder to open using cutting equipment and buys time.

2.1.10 Intruder alarms and verification systems

2.1.10.1 Consider using intruder alarms to monitor gates. Also consider using movement detectors. Make sure they are not set at too sensitive a level, but can still detect, for example, someone ramming the depot gates.

2.1.10.2 Operators should be aware that the Police are increasingly refusing to respond to alarms from commercial premises with a history of false alarms, unless the presence of an intruder is verified. There are various means of doing this and a number of intruder verification systems are on the market.

2.1.10.3 A pinhole camera typically situated by a gate or other likely access point can be triggered by an intruder breaking the beam from the alarm system. When activated, this sort of system will take photographs at short intervals.

2.1.10.4 Other systems work from existing equipment. For instance, you can buy software that connects intruder alarms to a standard PC, laptop, tablet or smart phone. When an intruder breaks the beam, the software accesses whichever camera has a view of the area. The footage can then be reviewed from any location where there is a suitable internet connection.

2.1.10.5 BS4737 covers basic alarm systems for premises and BS7042 covers high security intruder alarm systems.

2.1.11 Site illumination

2.1.11.1 Good illumination is an essential security measure for depots as well as having health and safety benefits. A well-lit perimeter fence, free of concealing vegetation, is a good starting point. The Regulations require areas where dangerous goods are stored to be (Capable of being) well lit.

2.1.11.2 Security lighting:

- deters entry into the area;
- conceals guards and their activities;
- aids visual observation by patrolling guards;
- supports CCTV surveillance;
- illuminates access point(s); and
- makes vehicle searches easier.

2.1.11.3 Illumination must balance the desire for security with the nuisance that excessive lighting may cause in environmentally sensitive areas.

2.1.12 Camera surveillance

2.1.12.1 Camera technology is improving all the time. In theory, CCTV installed alongside

beam movement activators is an excellent means of monitoring a depot. But there are a number of aspects that you need to look at before making any significant investment.

2.1.12.2 Consider hiring a consultant rather than relying on the installer's advice. This way you will get a system that suits your needs and you avoid the risk of over-specification.

2.1.12.3 It is vital that a company has the resources to monitor cameras on a 24-hour basis or at least sets time aside to check recordings. Where cameras are continuously monitored, make sure that monitors are constantly in view of the responsible person and not blocked in any way. Equally, make sure that other staff and visitors cannot see the monitors, and discover the limits of the cameras. CCTV will only be effective if you make sure that cameras give the best possible coverage and that recording equipment is working correctly.

2.1.12.4 If necessary, move cameras regularly so that blind spots do not develop and become known. Modern digital recording facilities now provide far better images, so use them wherever possible.

2.1.12.5 Pan tilt zoom cameras are good for focusing on particular areas. They consist of a moveable camera with a protective cover which allows the user more flexible monitoring.

2.1.12.6 Dome cameras can have advantages over pan and tilt cameras as they cover a much bigger area. They also make it difficult for intruders to tell whether the camera has picked them up.

2.1.12.7 Consider using fixed cameras on external walls. These are cheaper and there is less to go wrong than with dome or pan and tilt cameras. An ideal system for companies with a limited budget could involve a mixture of camera types.

2.1.12.8 Cameras set on towers are more versatile than cameras on buildings and will often be preferable to them. Again, dome cameras in such positions will provide the most effective scan of the whole site and can have additional benefits as a management aid. For instance, a dome camera will allow surveillance without showing where it's looking.

2.1.12.9 Still frame cameras activated by beam movement detectors are an alternative to video cameras.

2.1.12.10 It is also important to ensure that a reputable company services cameras regularly. There are many companies specialising in service contracts for this sort of equipment. Carefully check the condition of the material protecting the lens. The covering is there to protect the camera from weather damage, but it can itself become damaged over time, distorting the camera's view.

2.1.12.11 Intruders will often try to avoid detection by pointing cameras skywards, but they may not do the same to cameras on adjacent properties. Consider having a reciprocal arrangement with neighbouring companies. If your premises are located

on an industrial estate with limited entry/exit points, consider using cameras covering these points, funded either by companies on the estate or as a joint initiative with the local council. Take care with all cameras near residential sites to avoid any invasion of privacy.

2.1.13 Guards

2.1.13.1 Many companies use in-house guards. The main advantage is employee loyalty, but of course there are disadvantages too. This sort of guarding is expensive and you will need several guards to provide 24-hour security. This is a fixed cost to be balanced against other requirements.

2.1.13.2 Security could suffer because of the guards' familiarity with colleagues. For the same reason, in-house guards may find 'on-the-spot' searches of their colleagues more difficult than contract guards. If you choose contract guarding, be alert to the vulnerabilities linked to this option, even when using a well-established firm. There is a danger that contract guards will not know enough about your company's operation and so will fail to recognise risks. If possible, arrange for a pool of guards exclusive to the company who can then become familiar with it.

2.1.13.4 Some security companies provide travelling guards. Typically they visit premises three times a night. It is important to have a modern clocking-in system so that you can verify when the guards arrived at the premises and how long they stayed. The guards should, of course, vary the times of their visits and they should not build up a routine, as it will soon become obvious to criminals. It is also important to ensure that guards are aware of what may be missing from the site.

2.1.13.5 In an emergency, the security company should also be able to contact the key holder as soon as possible. The longer the incident reporting process takes, the more time the criminals have to get away and the less likely it is that losses will be recovered.

2.1.14.6 If you do decide to use third party security, it is important that the contractor provides good quality staff. Check the security company's recruitment procedure.

2.1.15 Raised road blocks and barriers

2.1.15.1 Raised road blocks are a highly effective means of preventing vehicles entering or being driven away without authority but they are very expensive. They must be fitted correctly as the repetitive raising and lowering can break concrete surrounds. Regular checks and maintenance of road blocks are essential and they should be constantly monitored to ensure that legitimate traffic is allowed through.

2.1.15.2 Many companies use barriers, which are adequate for low risk sites, particularly when they are manned 24 hours. However, most types of barrier can be lifted manually and so offer only limited security.

2.1.16 Key control

2.1.16.1 Parked vehicles should be locked when at base and the keys kept in a lockable container, these should have ‘locked’ as the default setting. This can either be a key case where any missing keys can be noted at a glance or, if required, a secure metal cabinet. Duplicate keys should have similar protection. Remember that the room in which keys are secured should also be protected from unauthorised personnel.

2.1.16.2 It is very important to have an issuing system, with regular checks on where keys are. If operating from lock-up premises (that is, non-24-hour), it is vital to monitor who has the entrance keys.

2.1.16.3 Keep the number of staff aware of security arrangements to a minimum. Where possible nominate a limited number of key holders, who should be able to reach the site quickly.

2.1.16.4 If keys are lost, change locks at once or exchange the vehicle with a similar one kept at another location.

2.1.17 Additional notes on site security

2.1.17.1 There are a number of bad practices that can make a depot less secure. For example, pallets stored against fences provide criminals with a ready-made ladder. By the same token, do not leave the yard shunt vehicle or any other heavy equipment where it is easily accessible. Criminals could use it to ram fences or break through gates.

2.1.17.2 Often, trailers are left attached to the prime mover when parked up in depots. On the one hand this can make the criminals’ job much easier. However, if an adequate immobiliser is fitted to the drawing vehicle, the criminals’ job can be made more difficult. If the criminals bring a tractor unit to take a semi-trailer away, an immovable tractor unit attached can frustrate them.

2.1.17.3 When trailers are disconnected from the units they could be secured with king pin or trailer leg locks. Consider leaving empty curtain-sided vehicles parked with the curtains open. This could deter criminals from slashing expensive curtains to see what is inside.

2.1.17.4 On-the-spot searches of vehicles and staff entering or leaving depots are accepted features of many operations. A vehicle seemingly on a routine journey could be removing goods without authority.

ANNEX 3: SECURITY ADVICE - ROAD VEHICLE & JOURNEY

3.0 Security on the road

3.01 Before taking control of a vehicle, drivers should consider security along with their normal daily safety inspection to make sure that, for example, the vehicles have not been tampered with. Drivers should make security checks part of their pre-journey safety checks and whenever they have left their vehicle unattended.

3.02 Drivers should report anything unusual to their Manager and, if appropriate, to the Police. The sort of things they should report include any irregularity in loading, locking or sealing, or in documents, changes in delivery instructions, or suspicions about people or vehicles.

3.03 The driver must carry a formal identity document with a photograph. If there are additional crew members in the vehicle, then they too should carry a formal identity document with a photograph.

3.04 Types of identification may include a driving licence, vocational qualification, passport or a photo ID issued by the employer or other organisation.

3.05 Where this is a change to current practice, inform all organisations making regular deliveries/collections to the site.

3.06 All DVSA examiners that are trained to deal with dangerous goods vehicles will be authorised to inspect for security at the roadside. Any non-compliance issues will be dealt with by seeking advice (by telephone if necessary) from the Department for Transport.

3.07 If not already implemented as part of the security plan or security risk assessment, then drivers should be advised to take the following precautions:

- remove the ignition keys, lock the cab doors and the vehicle's load space and switch on any alarm or immobiliser whenever they have to leave the vehicle unattended – even when going to pay for fuel or making a delivery (in some circumstances this may be impractical, such as delivering bulk fuels or gases. In which case consider fitting interlock braking systems, utilizing spare door keys or remote central locking);
- refuel on site before setting off whenever possible;
- pre-plan their route and avoid stopping for any reason. The driver should minimise stops by stocking up on anything needed for the journey before setting off;
- never leave windows open when away from the vehicle;
- where possible, use pre-planned, secure overnight parking facilities that are suitable for the dangerous goods being carried (especially high consequence dangerous goods). Drivers must follow the parking hierarchy specified in the ADR Regulations;
- particularly avoid using insecure, casual parking places as a routine practice;
- lock all doors while sleeping in the cab;

- never carry unauthorised passengers;
- never leave the vehicle unattended in a secluded or unlit area at night. Try to keep the vehicle in sight and be able to return to it quickly if it must be left unattended;
- contact base whenever they encounter any delay, problem or change in consignment details. The driver should not change the pre-agreed routing without prior confirmation from base; and
- never leave trailers or containers unattended. They should only be left in pre-agreed parking areas with approved security devices fitted.

3.08 If drivers hold the keys to their vehicle when not at work, they should:

- keep them secure at all times;
- never hide them for collection by a relief driver;
- never leave them where they could be copied; and
- make sure there is no way of identifying the keys or the truck from the key ring.

3.09 Drivers whenever possible should keep their cab doors and windows closed and locked throughout the journey.

3.10 The point at which high consequence dangerous goods are most vulnerable is when the driver is not with the vehicle. They should try to stay with the vehicle at all times unless a competent person supervises it.

3.11 Drivers should be instructed not to stop on the road unless required to do so by a Police or DVSA officer in uniform. If suspicious of the identity of the person who has stopped them, the driver could then display a 'dangerous load' card issued by the DfT [See section 3.3.1.3.] and talk to the officer through a closed window. Drivers should not get out of their vehicle until they have independently verified the officer's credentials.

3.1.1 Vehicle parking

3.1.1.1 Transport companies frequently look for details of lorry parking facilities around the country to park their vehicles whilst they are on route, particularly 'secure' parking. This is a difficult issue, for several reasons.

- There is no agreed definition of a 'secure lorry park', even among the Police and the insurance industry.
- There are no formal standards for assessing the level of security at a lorry park, or its effectiveness.
- The availability and quality of security measures and other facilities at a lorry park can change rapidly.

3.1.1.2 The Department for Transport does not currently publish a list of secure lorry parks. However, we can provide the best information available from advertised lorry parking facilities. These are listed on the International Road Union (IRU) website www.iru.org (search 'TRANSPark').

3.1.1.3 The Department for Transport wishes to emphasise that you should satisfy yourself regarding the level of security at a particular lorry park.

3.1.1.4 Vehicle operators and drivers must refer to the specific mandatory attendance and supervision requirements in the Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations and ADR chapters 8.4 and 8.5 as follows;

8.4.1 Vehicles carrying dangerous goods in the quantities shown in special provisions S1 (6) and S14 to S24 of Chapter 8.5 for a given substance according to Column (19) of Table A of Chapter 3.2 shall be supervised or alternatively may be parked, unsupervised, in a secure depot or secure factory premises. If such facilities are not available, the vehicle, after having been properly secured, may be parked in an isolated position meeting the requirements of (a), (b) or (c) below:

(a) A vehicle park supervised by an attendant who has been notified of the nature of the load and the whereabouts of the driver;
(b) A public or private vehicle park where the vehicle is not likely to suffer damage from other vehicles; or
(c) A suitable open space separated from the public highway and from dwellings, where the public does not normally pass or assemble.

The parking facilities permitted in (b) shall be used only if those described in (a) are not available, and those described in (c) may be used only if facilities described in (a) and (b) are not available.

8.4.2 Loaded MEMU's (Mobile Explosive Manufacturing Units) shall be supervised or alternatively may be parked, unsupervised, in a secure depot or secure factory premises. Empty uncleaned MEMU's are exempted from this requirement.

3.2.1 Communications – high consequence dangerous goods

3.2.1.1 Mobile communications help to prevent crime. They allow the driver to contact base on arrival at an unoccupied site or to report any suspicious activities.

3.2.1.2 Mobile communications also allow the carrier to keep track of routes and any overnight parking sites used.

3.2.1.3 Vehicles should be fitted with radios or some other means of two-way communications between the driver and the base. Panic buttons can be fitted which a driver can press if under duress, possibly in a hijack situation. This will send an alert to the operator so the Police can be contacted.

3.2.1.4 Instruct the driver to communicate with their operating base at frequent and regular intervals. They should say where they are, what route they are taking and, if appropriate, their estimated time of arrival at their next destination together with confirmation that everything is in order.

3.2.1.5 Instruct the driver to alert base to any unusual or suspicious activities. Consider giving the driver a password to use when raising the alarm.

3.3.1 Dangerous load cards – high consequence dangerous goods

3.3.1.1 Drivers carrying high consequence dangerous goods may consider carrying a dangerous load card. It does not specify the vehicle, the driver, or the type of high consequence dangerous goods being carried. A carrier would need to hold enough cards to cover the maximum number of vehicles carrying high consequence dangerous goods at any one time.

3.3.1.2 A driver should only produce this card if they are stopped by a Police or DVSA officer **and are suspicious** about the validity of the officer. The card tells the Police and DVSA that the driver will not open the vehicle until the officer's identity has been verified; Police and DVSA have approved this procedure. The carrier will need to decide if any load is of high consequence, based on information provided by the consignor.

3.3.1.3 You can download the dangerous load card and print as many as you need from the DfT website via this link:
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/338874/dangerous-load-card.pdf

Please note that cards no longer carry a unique serial number and there is no longer a requirement to report a card lost or stolen.

3.3.1.4 Operators should be aware that for their vehicles to be part of the scheme they should ideally have:

- in-cab communications; and
- a working tracking system, where fitted.

3.3.1.5 Their company should also have an up to date Security Plan.

3.3.1.6 Where the driver is suspicious of the identity of the person who has stopped his/her vehicle, the driver should:

- stay in the cab, make sure the doors are locked, and put the parking brake on;
- display the dangerous load card;
- if in contact with the operating centre, stay in contact;
- give the operating centre full details of the vehicle's location and the reason why it has been stopped;
- ask the stopping officer for identification (talk through the closed window);
- dial 999 (if genuine, the officer should also inform the force control room of the stop);
- tell the Police control room they are carrying dangerous goods, giving the location and identity of the stopping officer; and
- if the Police control room confirms it is a legitimate stop, comply with the instructions of the stopping officer.

3.4.1 Secure vehicles

3.4.1.1 Vehicles may be secured by means of a range of additional security measures. Consider the following.

- Use security equipment, it will make vehicles less attractive to criminals. Discuss this with insurers, including 'goods in transit' insurers, vehicle dealers, transport security consultants and security equipment manufacturers.
- Have security equipment regularly checked by the installer.
- Each vehicle will need different levels and types of security equipment, depending on its use. All vehicles should have some form of immobilisation, if the manufacturer has not already fitted this.
- When buying vehicles, consider the security equipment already fitted and what extras could be added.
- Your insurer and the Crime Prevention Team from the local Police can provide specific security advice.
- Trucks are stolen whatever their load might be.

3.4.1.2 Vehicle manufacturers are producing increasingly sophisticated anti-theft equipment, often running off the vehicle management system.

3.4.1.3 Equally, criminals are becoming more ingenious. If nothing else, this has raised the quality of vehicle security systems to a level that will defeat the opportunist criminal providing these systems are armed.

3.4.1.4 Many anti-theft devices are self-arming and do not rely on the driver remembering to set them. Some equipment gives the driver about 30 seconds to leave the cab after switching off the engine and removing the key from the ignition, and then sets itself automatically. The system will remain armed until de-activated by a high security key, electronic touch sensors or a 'smart card'.

3.4.1.5 Vehicle manufacturers now fit alarms and immobilisers as standard. This has reduced the number of thefts by opportunists and is often emphasised by manufacturers in the marketing of the vehicle.

3.4.1.6 Insurers have been increasingly proactive in the specification of anti-theft equipment in commercial vehicles. The insurance industry's testing facility at Thatcham produces a list of approved security devices, further information can be found at their website via the following link. https://www.thatcham.org/security

3.5.1 Physical vehicle security

3.5.1.1 Physical security of commercial vehicles can take the form of additional or stronger high security locks, grilles and the like. It may give either independent security or complement an alarm system. Taken in isolation, physical security can offer a simple and cost-effective solution in low risk situations. It can also be a strong deterrent to the opportunist attacker.

3.5.1.2 Many security locks depend on the driver to operate them manually. 'Slam locks' can be fitted to load space access points in commercial vehicle bodies. They are popular

with parcel carriers involved in multiple drops. Drivers only have to close the door and the load is automatically secure. However, any security is only as good as the weakest point.

3.5.1.3 The purpose of a bulkhead dividing the driver/passenger area and the load compartment in panel vans is to isolate goods in the load compartment. For example, a bulkhead fitted in a panel van means that access is only through the side or rear loading doors, which can be secured with additional locks.

3.5.1.4 Bulkheads come in a variety of materials, such as solid steel, plywood or steel mesh. Correctly fitted mesh bulkheads can give adequate security but still allow thieves to see the goods and may therefore make a break-in more likely. Solid bulkheads are better.

3.6.1 Immobilisers

3.6.1.1 Immobilisers aim to render the vehicle or trailer immovable. Immobilisation systems can be used in isolation or integrated into an alarm system. Virtually all insurance approved alarm systems will incorporate, as standard, some form of immobilisation as part of the overall security system.

3.6.1.2 When choosing an immobilisation system, take into account:

- vehicle type;
- the risk to both vehicle and load; and
- loading and unloading.

3.6.1.3 Wheel clamps are an effective form of immobilisation, especially on the smaller wheels of light commercial vehicles. Wheel clamps for large commercial vehicles are heavy and cumbersome. Drivers have to fit them and lock them into place, so the risk that they either won't fit them, or that they will fit them incorrectly (particularly at night), is higher than for other vehicle immobilisation devices.

3.6.1.4 To immobilise an articulated trailer, kingpin or trailer leg locks are the most common and effective way. Kingpin locks are a heavy hardened steel clamp or cover, which fits round or over the kingpin and locks it in position. It makes it impossible for the kingpin on the trailer to be coupled with the fifth wheel coupling on the tractor unit. Fitting kingpin locks can be a difficult and dirty job. Trailer leg locks are an alternative. Both kingpin and trailer leg locks are manually operated devices so the driver has to put them on and lock them into position.

3.7.1 Alarms

3.7.1.1 Immobilisation does not stop a criminal from vandalising a vehicle or unloading it where it stands. Alarm systems do two things:

- they create a loud sound that provides both a warning and a deterrent; and
- when fitted in conjunction with a vehicle immobiliser, they 'buy time'.

3.7.1.2 When selecting a vehicle alarm, consider whether you want it to be:

- manual (set by driver) or automatic (self-setting at all times); or
- powered by the vehicle's own battery only or by the vehicle's battery with a back-up facility.

3.7.1.3 An alarm system powered off the vehicle's own battery may be perfectly sufficient for light commercial vehicles in low risk operations, where the battery is locked under the bonnet. Large commercial vehicles with exposed batteries on the chassis require a back-up facility for alarm systems. There is little point in having an alarm system that can be rendered inoperable merely by disconnecting the battery terminals.

3.7.1.4 Key switches turn a system on or off (automatic systems 'pulse' to allow the driver to re-enter the cab or to unload). It is important to use good quality security key switches/pulse devices with a large number of combinations.

3.7.1.5 In the case of high risk loads, independent alarm security may be fitted to the tractor unit and the trailer, tank or container. Where a single shared alarm system covers the tractor and the trailer, tank or container when they are coupled, the back-up battery may be on the trailer, tank, or container. It provides independent protection when the trailer, tank, or container is free-standing. However, this may leave the tractor without any alarm protection at all when separated. In this case, it is important to immobilise the tractor.

3.8.1 Tracking systems

3.8.1.1 Vehicle tracking systems are not, strictly speaking, anti-theft devices. But they can help in deterring theft and recovering vehicles, where time is often of the essence. Use transport telemetry or other tracking methods or devices to monitor the movement of high consequence dangerous goods where appropriate.

3.8.1.2 Some tracking system manufacturers offer 24 hour monitoring via a movement sensor linked to the tracking unit. The system manufacturer is then able to alert the owner if the vehicle is illegally moved. This means a faster response to theft. Some on board tracking systems offer additional features, which can monitor the product levels in tankers for example. These enable the operator to have live visibility of the vehicles' location as well as the quantity of product unloaded. Portable tracking devices are available that can be fitted into a load space, a shipping container for example, which can send an alert if the doors are opened.

3.8.1.3 Certain tracking systems offer additional features, including:

- remote vehicle immobilisation;
- door opening recording;
- panic alert systems; and
- geo-fencing facilities.

3.8.1.4 Geo-fencing constantly monitors the vehicle on a predetermined route or at a known location. Any unauthorised movements will automatically trigger an alert.

3.8.1.5 Telematics systems offer proven vehicle management benefits, as well as improving

security. The benefits include better fuel consumption, enhanced safety and cheaper maintenance. These benefits often mean that telematics systems pay for themselves relatively quickly.

3.9.1 Cameras on vehicles

3.9.1.1 Cameras are regularly used on the back of goods vehicles to help the driver manoeuvre the vehicle. These are also a valuable covert measure to monitor the security of the load. More frequently now, forward-facing cameras are being fitted.

3.10.1 Roof markings

3.10.1.1 These help Police air support units to identify stolen vehicles. The Department for Transport encourages hauliers to use roof markings, particularly those who regularly carry high consequence dangerous goods.

3.11.1 Vehicle and trailer records

3.11.1.1 Details of vehicles, trailers and loads should be available quickly in case the Police need them. As a minimum, record the following:

- vehicle registration number/trailer serial number;
- make & model;
- body type, for example, dropside, flat bed, curtainsider, solid box, tanker;
- vehicle identification number (VIN);
- engine number;
- gear box number;
- other identification numbers, marks and livery details;
- number of axles;
- special equipment fitted (with serial numbers);
- security devices fitted; and
- mileage.

3.11.1.2 Photograph vehicles and items of plant from the front, side and rear. This will help Police in issuing descriptions and looking out for the stolen property. You may wish to consider putting roof markings on the vehicles as this can dramatically improve the chances of the vehicle being spotted from police helicopters.

3.11.1.3 Keep a daily record of each vehicle's movements with precise details of the load and the driver on each occasion. Also note other staff who come into contact with the vehicle or its load, such as the person who loads the goods.

ANNEX 4: SECURITY ADVICE - MANAGEMENT PROCEDURES

4.0 Procedures

4.01 This section highlights effective measures which organisations involved with the transport and temporary storage of dangerous goods can take to improve security procedures. Incidents sometimes occur because of a failure to recognise risks and adopt basic security measures.

4.02 Employers must consult all their employees, in good time, on matters which affect their health and safety. In workplaces where a trade union is recognised, this will be through union health and safety representatives. In non-unionised workplaces employers can consult directly or through other elected representatives.

4.03 Make sure that you have clearly formulated standards of responsibility and performance. These need to be understood and accepted by everyone involved in operations. You could instruct new staff in the security measures applicable to their duties as part of their induction training.

4.04 Check regularly that drivers understand and use any security equipment fitted to their vehicles. The same goes for security equipment on premises. DfT recommend companies incorporate these principles into staff training and development programmes.

4.05 Arrange regular checks to ensure that all security equipment and control measures are functioning correctly. Above all do not ‘fit and forget’.

4.06 Keep up to date with current security developments and discuss any problems with the company’s security manager (where there is one), local Police contacts and others in the industry. Make use of actual events, root cause analysis and the experience of others.

4.07 Operators should continually review and refine their security procedures.

4.1.1 Dangerous Goods Safety Adviser (DGSA)

4.1.1.1 ADR & RID Chapter 1.8.3 requires that each undertaking, the activities of which include the carriage, or the related packing, loading, filling or unloading, of dangerous goods by road and/or rail, shall appoint one or more safety advisers for the carriage of dangerous goods, responsible for helping to prevent the risks inherent in such activities with regard to persons, property and the environment.

The main tasks of the DGSA are;

- Monitoring compliance with the requirements governing the carriage
- Advising on the carriage of dangerous goods
- Preparing and producing an annual report to the management

4.1.1.2 For security, they are required to ensure a security plan is in place when required. Further tasks of the DGSA are listed in ADR & RID Chapter 1.8.3.3.

The DGSA is effectively an auditor for all these items to ensure good order is maintained, they may or may not be the appointed person for security and thus may or may not be the author of the security plan(s)

4.2.1 Management routines and secure working practices

4.2.1.1 You should carry out and document a security risk assessment of your operational procedures. Although this is not as detailed as a Security Plan, it is a methodical review of your operations to minimise any risk of action against you. You should record any action taken to reduce the risk and disseminate it to the appropriate staff. You should regularly review operational procedures.

4.2.1.2 Even if your organisation does not store or carry high consequence dangerous goods there are a number of routines that you can adopt to improve security.

- keep documentation about loads in a secure place, criminals could use consignment documentation to show they have title to the goods;
- keep all vehicle/premises keys in a secure place.
- where possible, vary routes and drivers to avoid regular patterns developing;
- keep in regular touch with local Police crime desk, local Intelligence Officer or Counter Terrorism Security Adviser (CTSA);
- instruct drivers to secure the cab and where appropriate the load compartment. Where possible, they should lock cab doors when loading or unloading;
- advise drivers not to talk about their load or intended route in a public place or over the radio. They should be careful when asking people for directions or advice on off-road parking; and
- advise drivers to be aware of deception at delivery points or on route.

4.2.1.3 Use security seals on vehicles, tanks or containers where appropriate to protect the load. Seals quickly reveal any attempts at tampering through a pre-determined number code or a randomly generated digital seal number. More expensive seals are specially made to withstand violent attack.

4.2.1.4 Criminals may try to obtain vehicles with your company's livery and staff uniforms as a means of claiming authority to collect goods and/or vehicles. When disposing of vehicles, remove all identifiable livery.

4.2.1.5 Use the vehicle registration document to tell DVLA of changes to livery and major components. Pass disposal details relating to scrapped or written off vehicles to DVLA immediately.

4.2.1.6 Consignors should offer dangerous goods only to carriers that they have appropriately identified. This should be done in advance of any physical movement of goods. If high consequence dangerous goods are being carried, you should be satisfied that the carrier has proper security measures in place. The same would apply to carriers that subcontract the work on.

4.2.1.7 In general, you should strictly monitor the storage, issue and return of staff uniforms. When staff leave or exchange uniforms, they should return their old uniforms. Take care when issuing staff uniforms to temporary workers.

4.2.1.8 Sites receiving or consigning high consequence dangerous goods should:

- schedule vehicle deliveries or collections, wherever possible, so that the arriving vehicle can be cross referenced against the expected vehicle schedule held at the gatehouse; and
- identify the driver and vehicle and give the customer/receiver an estimated time of arrival, which should be within a reasonable period of the intended delivery time.

4.3.1 Communication with staff – high consequence dangerous goods

4.3.1.1 Make sure that all staff involved with the transport of high consequence dangerous goods understand the need for robust security measures. Employees are more likely to be reassured than alarmed by such.

4.3.1.2 Open communication allows all staff to report anything suspicious. Consider a 24-hour confidential reporting line.

4.3.1.3 Investigate any reports of suspicious behavior and report them to Police by dialing 999, Crime Stoppers 0800 555111 or the Police non-emergency number 101. Call the Anti-Terrorist Hotline 0800 789 321 with any tip offs and confidential information.

4.3.1.4 In certain highly sensitive operations, you may need more formal surveillance systems. Deploy such systems with great sensitivity.

4.4.1 Cyber Security

4.4.1.1 Almost every business relies on the confidentiality, integrity and availability of its data. Protecting information, whether it is held electronically or by other means, should be at the heart of the organisation's security planning.

4.4.1.2 The key questions to keep under constant review are:

- Who would want access to our information and how could they acquire it?
- How could they benefit from its use?
- Can they sell it, amend it or even prevent staff or customers from accessing it?
- How damaging would the loss of data be?
- What would be the effect on its operations?

4.4.1.3 The Centre for the Protection of National Infrastructure provides a range of guidance documents and technical notes aimed at improving practices and raising awareness of current issues related to information security on their website.
http://www.cpni.gov.uk/advice/cyber/

4.4.1.4 Several Government Departments have combined to produce a guide showing businesses the practical steps they can take to improve the security of their networks and the information carried on them.
https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-summary

4.5.1 Carriage of Explosives (ADR)

4.5.1.1 The Carriage of Dangerous Goods and Use of Transportable Pressure Equipment Regulations 2009 section 7 places specific security requirements for carriage of goods in hazard class 1. These are more prescriptive than the requirements set out in ADR Chapter 1.10.Refer to the aforementioned section 7 for full details.

4.5.1.2 Even though these requirements are in place, carriers and consignors will still need to ensure they meet all of the requirements of ADR chapter 1.10. You should not store explosives temporarily at berthing areas, vehicle depots or storage terminals unless the site is licensed or registered for that storage.

4.5.1.3 The Health and Safety Executive (HSE) and the Department for Transport have agreed the division of roles and responsibilities in respect of the security of explosives during the entire transport logistics chain.

4.5.1.4 Also, if you handle Division 1.4 explosive material that if misused could contribute to or cause large loss of life or damage to the economy or environment, then it is strongly recommended that you treat this material as high consequence dangerous goods.

4.6.1 Carriage of Ammonium Nitrate

4.6.1.1 Solid Ammonium Nitrate based fertiliser is classed as dangerous goods. It is subject to a separate Code of Practice. https://www.aictradeassurance.org.uk/latest-documents/transfer-traceability-fertiliser-classified-as-dangerous-goods/
This Code is designed to minimise the physical transfer of product, as defined, and make it easier to trace for security purposes. This is being achieved by placing the responsibility for the distribution/delivery of the product to the farmer, the producer, or the first importer or his appointed distributor. The measures detailed in the Code apply equally to all parties.

4.6.1.2 The National Counter Terrorism Security Office (NaCTSO) offers detailed advice to farmers, growers, land-owners and farm staff on how to store fertilisers securely. https://www.gov.uk/government/publications/secure-your-fertiliser/secure-your-fertiliser

4.6.1.3 The Agricultural Industries Confederation manage the voluntary Fertiliser Industry Assurance Scheme (FIAS). Further information can be found on their website: www.agindustries.org.uk

ANNEX 5: SECURITY ADVICE - PEOPLE & TRAINING

5.0 People

5.01 Personnel security plays an important part in any integrated approach to protecting a business from threats, including terrorism. Workforce security can raise difficult and sensitive issues for employers and managers, as well as for individual employees. Any measures taken need to be proportionate to the perceived risks. A review and risk assessment of workforce security systems should be part of a risk management approach to security.

5.02 Any person engaged in the transport of dangerous goods should consider security requirements according to their responsibilities. Everyone should be aware of the potential for misuse of dangerous goods and follow the requirements of the regulations according to the level of their responsibility.

5.03 Many external threats to a business or organisation depend to some degree upon the co-operation of an 'insider'. This could be a permanent or temporary employee. It could be contract or agency staff, such as a driver, cleaner, caterer or security guard, who is given access to business premises. 'Insiders' may be recruited from among existing staff, or they may be new staff deliberately infiltrated into the business. When considering the security of your operation and the responsibilities staff are given, it is important that people are suitable for the post.

5.04 Check the credentials of new employees and contractors or agency staff. You can do this directly when you draw up an employee's contract of employment, or indirectly with contractors as part of an overall Service Level Agreement.

5.05 Businesses and organisations should build security responsibilities into every employee's contract of employment, including information security. A security function should also feature in the job description of every employee involved in the transport of dangerous goods.

5.06 Many factors will affect the level of risk of an employee or contractor exposing details about the vulnerabilities of the organisation to a third party, including:

- transport information;
- the nature of the operation;
- the types and quantities of dangerous goods;
- journey, consignor or consignees details; and
- access to the site.

5.07 The key question in relation to workforce security is:

Are the people in the workplace who they say they are, and should they be there?
Personnel security advice is available at the CPNI website via the following link *http://www.cpni.gov.uk/advice/Personnel-security1/*

5.1 Recruitment

5.1.1 Appropriate persons

5.1.1.1 Reliable and responsible staff are central to making sure that other security measures work effectively. Warn applicants that giving false information, or failing to disclose material information, would be grounds for a refusal or dismissal.

5.1.1.2 Organisations should ensure all new employees who are to be involved with the transport of dangerous goods are suitable for the task and that they hold verifiable:

- licences, certificates and operating documents where applicable; and
- permission to work in the UK where necessary.

5.1.1.3 Licences, certificates and operating documents that staff may need to do their job should be checked at regular intervals.

5.1.2 Pre-employment checks (all staff including self-employed)

5.1.2.1 Check the employment record of everyone that needs to be involved in the transport of dangerous goods. Obtain documentary evidence of background, experience and character for all potential employees. Insist on original documents to check identity and qualifications.

5.1.2.2 Ask the candidate for the following information:

- full name, address and date of birth;
- National Insurance or other unique personal identifying number where appropriate;
- details of any past criminal convictions by requesting a disclosure certificate (where this is allowed by law); and
- full details of references (where applicable).

5.1.2.3 Obtain a continuous record of the applicant's education and employment history. This may not always be easy, but in general ask for information covering the preceding 10 years, and as an absolute minimum covering the previous five years.

- When checking references by phone, obtain the number you need from a telephone directory or enquiries service. Any number supplied by an applicant could be that of an accomplice.
- Do not accept open references such as 'to whom it may concern'.
- Obtain confirmation in writing from employers, educational authorities, and so on.
- Insist on seeing the applicant's original birth certificate, not a photocopy. Obtain a recent photograph of the applicant and get him/her to sign it in the presence of a company representative.

5.1.2.4 Check identities by asking to see a passport, an official photo ID and utility bills sent to the applicant's address and so on. Where appropriate, you should also verify proof of right to live and work in the UK.

5.1.2.5 A driving licence contains important personal information about the holder. Ask the applicant for their date of birth. Compare the stated date of birth against the birth certificate. Check driving licences thoroughly using the DVLA licence checking service. Check for endorsements regularly. Photocopy the licence, ADR qualification and Driver CPC and keep copies on file.

5.1.3 Existing employees

5.1.3.1 There are obvious sensitivities when it comes to your own staff. In the vast majority of cases, your employees will have exemplary employment records. And apart from the issue of sensitivity, both employee and employer will be bound by a contract of employment.

5.1.3.2 You will need to check that existing employees who work on sensitive sites are suitable to carry out their responsibilities in order to ensure the integrity of the overall system.

5.1.3.3 You should ensure that you have on file the existing employee's

- full name, address and date of birth;
- National Insurance or other unique personal identifying number where appropriate; and
- copy of their passport or photographic drivers licence (if one is held).

5.1.3.4 In some cases this information may not have been obtained at the time the employee took up employment, may have been discarded, or may simply have become out of date. You need to check and update it regularly.

5.1.3.5 It is good practice to produce a Security Policy Statement. This should set out the general principles for the secure operation of organisation and the serious view taken of dishonesty, irresponsibility or negligence. You might wish to display this on the notice board.

5.1.4 Contractors (including providers of temporary staff)

5.1.4.1 Many organisations use contractors or agencies to provide a growing range of services, including additional resources. It is imperative when dealing with high consequence dangerous goods that hauliers are appropriately identified and they can demonstrate they are regulated by the Department for Transport. They may also be part of a recognised industry accreditation or earned recognition scheme with the DfT.

When starting a business relationship with a new transport contractor, consideration should be given to auditing their systems or seeking written assurances for compliance with the security regulations. You should ascertain if there is a security plan in place when required and that there is a security training programme for their staff.

5.1.4.2 Contractors may create new vulnerabilities and expose organisations to a greater 'insider' threat than they would face if relying on directly recruited staff. Some contractors or agencies may be less rigorous in their selection procedures than those who use their services would be.

5.1.4.3 Contractors, including transport service providers, should undergo the same pre-employment screening processes with their employees, responsibility for implementing these checks will rest with the contractor. They should be able to demonstrate, from their records, that they have carried out these checks.

5.1.4.4 Organisations should consider additional checks or screening of contractors or sub-contractors employed in key positions, such as security guards at site access points. It is worth establishing whether a contractor or agency is part of a recognised professional organisation which accredits standards in that industry.

5.1.4.5 Good practice is to ensure that you have procedures to confirm that a person sent by a contractor or agency is indeed the individual who turns up.

• Require the contractor or agency to provide in advance a photo of the individual, authenticated by them. You can compare this with the person who turns up at your premises before you let them in.

• Require the contractor or agency to provide their own photo ID, which you can check on each entry.

• If you provide your own permanent staff with a photo ID, extend this to contract staff. Ideally you should retain these passes between visits. On each visit, compare the contractor or agency staff member with their photograph before handing them the pass.

• Have an agreed substitution procedure for contract staff that are temporarily absent. This could include setting out what is acceptable in terms of a temporary replacement, and considering whether to restrict their duties or access.

5.1.5 Employers

5.1.5.1 Employers can try to identify potential risks by encouraging both managers and staff to be alert to changes in employees' behaviour and attitudes. These might suggest potential conflicts of interest or disaffection that could undermine trust in them.

5.1.5.2 If you do have concerns, act sensitively. It is best to be as open as possible with the individual concerned and explore the issue in a constructive, non-threatening manner.

5.1.5.3 Employees must be given the confidence to report concerns and must know that their employer will take their reports seriously and treat them confidentially. Any action resulting from such reports must be in accordance with employment law, other legislation such as the Human Rights Act, the Public Disclosure Act, the Data Protection Act and best practice.

5.1.5.4 It is easier to monitor behavioural changes in your permanent staff than it is with contract staff, who may not be as well known to you. Employers should consider:

• providing permanent supervision, either throughout the period when the

contract/agency staff are on the premises, or when they have access to particularly sensitive or business critical areas; and
• nominating a permanent employee to be responsible for the contract staff as individuals, not just for overseeing delivery of the contract. This member of staff could then pick up on any concerns about potential conflicts of loyalties and the like, both with the individual and with the contractor/agency manager responsible for oversight of the contract.

5.1.5.5 If you are involved in high consequence dangerous goods then you will need to record in a security plan who is responsible for your security.

5.2 Training (all staff)

5.2.1 Security awareness

5.2.1.1 All businesses and organisations are required to provide security awareness training for everyone involved in the carriage of all dangerous goods. It is also a requirement to periodically supplement initial training with refresher training at suitable intervals. Training should be provided at the induction stage and supplemented with periodic refresher training.

5.2.1.2 People involved in the transport of dangerous goods need a basic level of training to improve their awareness of security. People involved in the transport of high consequence dangerous goods will need more detailed training as there are tougher security controls in place for these substances. Also, specific training may need to be given to drivers, operational staff and other relevant staff members that hold specific security responsibilities.

5.2.1.3 The training should deal with:

- the nature of security risks;
- recognising security risks;
- how to minimise security risks; and
- what to do in the event of a security breach.

5.2.1.4 The training should also include awareness of security plans (if appropriate). This should be at a level appropriate to the responsibilities of individuals and their part in implementing security plans.

5.2.1.5 The employer should record all security training and make the records available to the employee if asked. It is recommended that training records are kept for no less than four years.

5.2.1.6 You can find further guidance on dangerous goods security training on the DfT website via the following link.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/318451/dangerous-goods-road-training.pdf

5.2.1.7 The Department for Transport has produced (in 2015) a new training film titled ‘Lockdown’ to assist those involved in the carriage of high consequence dangerous

goods to provide security awareness training to all staff. DVD copies can be obtained free of charge to HCDG sites and carriers on request, please send your details to landsecurity@dft.gsi.gov.uk

The film has been designed to suit all types of organisation involved in the carriage of high consequence dangerous goods (HCDG). Most roles within any business have been featured and it is suitable to watch in a passive viewing environment or included as part of a classroom based training session. The film could be watched and form the basis of discussions as to how certain aspects might apply to any type of transport operation. There is an MP4 version of the film within the DVD for those trainers or companies that wish to utilise intranet systems or similar; there is also a PDF training notes document on the DVD for use as a hand-out.

General security training films have also been produced by the Centre for the Protection of National Infrastructure (CPNI). www.cpni.gov.uk

5.2.1.8 Security should be part of the daily routine for all staff, particularly those involved with the transport of dangerous goods. Train all staff in the right habits and make security part of their daily work.

5.2.2 Driver training – high consequence dangerous goods

5.2.2.1 The training programme for drivers who transport high consequence dangerous goods could include a driver's handbook or other document, which covers security measures and procedures for the vehicle, load and premises. The security section of the handbook or other document should point out that no unauthorised persons are allowed to travel in the cab and include guidance to drivers on preventing theft of their load by deception.

5.2.2.2 The drivers' instructions should include:

- how to use the security equipment fitted to the vehicle and at the premises, where appropriate;
- hijack awareness/avoidance; and
- a reminder to carry photo ID.

5.2.2.3 The driver's dangerous goods vocational training certificate exam will include questions on security.

5.2.2.4 Brief drivers on what to do in the event of hijack or criminal attack. Emphasise that they must not put themselves at risk in an attempt to protect the vehicle and load.

5.2.2.5 You may want to issue the prepared advice sheet for drivers attached at Annex 7 of this guidance.

Annex 6 Risk Assessment Template

RISK ASSESSMENT MATRIX

ASSETS		THREAT	VULNERABILITY	RISK STATUS (Threat x Vulnerability)	RISK IMPACT	SUMMARY OF COUNTER MEASURES
Vehicles	[insert text]	[insert text / colour]	[insert text / colour]	[insert text / colour]	[insert text]	[insert text]
Site & Buildings	[insert text]	[insert text / colour]	[insert text / colour]	[insert text / colour]	[insert text]	[insert text]
Information	[insert text]	[insert text / colour]	[insert text / colour]	[insert text / colour]	[insert text]	[insert text]
People	[insert text]	[insert text / colour]	[insert text / colour]	[insert text / colour]	[insert text]	[insert text]

EXPLANATORY NOTES

1. GENERAL

This risk assessment matrix is designed to be a simple reference document for all of your key assets. The entries for each box are explained below.

When completing the columns titled Threat, Vulnerability and Risk Status you might find it easier to use colours or simple words to identify the severity of the problem. A common scheme is the traffic lights colours: red, amber and green – where red stands for the highest severity.

Here is an example risk status with the different combinations of threat and vulnerability:

THREAT	VULNERABILITY	RISK STATUS
Low	Low	Low
Low	Medium	Low
Low	High	Medium
Medium	Low	Medium
Medium	Medium	Medium
Medium	High	Medium
High	Low	Medium
High	Medium	High
High	High	High

You can also use these colours to highlight the severity of the risk occurring.

2. ASSETS COLUMN

Vehicles

Vehicles or trailers used to transport dangerous goods. Not too much detail is required. It may just be two or three entries. For example large goods vehicles, trailers and light goods vehicles. Vehicles containing high consequence dangerous goods would attract a higher rating.

Site and buildings

The buildings, or rooms within the buildings, that actually contain the dangerous goods and where these buildings are situated. It need not necessarily apply to the whole site, just the critical area(s). Sites or parts of them storing high consequence dangerous goods would attract a higher rating.

Information

Information that identifies where dangerous goods are stored or can be obtained, or would make deception easier. This might include a security plan, schedules of journeys or drivers details.

People

Individuals or groups of people that handle or have access to dangerous goods (such as loaders, packers, contractors) who could steal the dangerous goods or information, or be coerced into helping the attack.

3. THREAT COLUMN

The perceived threat, the likely abilities of the attackers, the tools they may be expected to use, and the most likely methods of attack. This information would commonly come from the Land Transport Security Division at the Department for Transport. However, in the absence of any such information, you should complete this entry based on local knowledge. If nothing is known, enter it as low or colour it green. You should pay more attention to this aspect if you are involved in the transport of high consequence dangerous goods.

Perpetrators could include individuals or groups such as:

- terrorists
- other criminals
- political groups
- protestors
- those that are mentally unstable
- employees

4. VULNERABILITY COLUMN

This identifies the relative weaknesses of the asset. For example, vehicles may always be loaded and kept out in the open, the loading bay doors are always left open, and there is no fencing around the site or building.

5. RISK STATUS COLUMN

A rating that is a combination of the threat and vulnerability (see matrix above)

6. RISK IMPACT

What would be the consequence of the risk occurring? What would be the damage?

7. SUMMARY OF COUNTER MEASURES COLUMN

This would reflect the ratings given for the risk status and the risk impact. i.e. a low (green) rating for both the risk status and the risk impact could result in minimal security measures being implemented as opposed to a high (red) rating for both the risk status and risk impact which could result in high security measures being implemented.

ANNEX 7: DRIVER ADVICE SHEET

Introduction

It is estimated that eight out of every 1000 HGVs on the road are stolen every year and only one of those eight is recovered. More than half of all trucks are stolen from operators' own premises.

Your truck is your livelihood. The tips in this fact sheet will help you stop truck thieves. Please take the time to read this leaflet and discuss any questions you may have with your employer. Keep it safe in your cab for future reference.

If you witness suspicious or criminal behaviour, call the Police immediately by dialling 999. Always let your employer know what is happening. If you suspect terrorist involvement, then also call the Anti-Terrorist Hotline on 0800 789 321.

Be Secure

When you leave your vehicle, always lock it and always take your keys with you. Never leave them in the cab.

Always make sure whenever possible that your cab and, where appropriate, the load compartment are secure.

When loading or unloading, lock the cab.

When driving, where appropriate, lock the load compartment.

Check that all security devices are working.

If you keep the lorry keys when you are not at work:

make sure they cannot be identified – don't leave anything on the key ring that tells who they belong to or what vehicle they fit;

never leave them where strangers can see them; and

always keep them somewhere safe.

If you keep your keys at the operating centre:

make sure they are in a lockable place out of sight of strangers; and

never use a 'hiding place', for example, inside the front bumper.

The theft of vehicle keys is on the increase, so be warned!

Park Safely

Whenever possible decide where you are to park overnight before starting your journey.

Park your vehicle within sight and where you can return to it quickly for short breaks.

When returning, check all round for signs of interference, including any load security seals.

When returning to the UK from Europe, be particularly alert for signs of illegal immigrants and be aware of any special instructions at ports and the Channel Tunnel.

Plan Ahead

Plan your route beforehand. That way you will not have to stop to ask directions. If you know exactly where you are going, no-one can mislead you with wrong directions.

Be unpredictable in your daily work pattern.

Be Aware

Avoid talking about loads or routes with other drivers or customers (including over radios, phones or via social media).

Be cautious if you are forced to stop, for example, at the scene of an accident or an emergency, or at police stops.

If you are carrying a dangerous load card:

keep it safe; and

if you are stopped by the Police or DVSA and are suspicious about the validity of the officer, follow the instructions on the reverse of the card.

During security alerts, follow the advice given to you by local police. At these times only, make sure:

someone competent stays with your lorry; and

if you're alone, leave a clearly displayed note explaining how to be contacted.

Everyday Security

Avoid regular routes or stops for newspapers, cigarettes or meals – a recognisable pattern makes you an easier target for thieves.

Never give lifts; it is illegal to carry unauthorised persons when transporting dangerous goods.

Make sure you understand and use the vehicle's security equipment and check it's working properly.

Never leave keys in or on your truck.

If your truck or trailer has a roof marking and you are the victim of a crime, make sure you tell the Police.

Documents

When you collect a load:

check the load matches the collection note;

make sure it is clear where you are delivering to and who will receive the goods;

get a contact number if you can; and

record the load seal number, if appropriate.

When you deliver:

check the load seal is intact and the number is the same as on the delivery note;

check that quantities and weights match the collection and delivery notes;

make sure you are delivering to the right place (check collection and delivery against the notes);

if the delivery instructions are changed, get written confirmation of the changes from senior staff at the delivery address or from your employer; and

make sure that there is a clear signature and printed name on the POD (proof of delivery note).

Protect Your Own Belongings

Hide personal property from view.

Company Security

Your company security instructions and procedures are designed to protect your vehicle and its load. Follow them at all times.

If you fail to follow them, your employer could take disciplinary proceedings against you, the driver.

Remember, if you lose your truck, you could lose your job.

If you see anything suspicious, report it to the Police by dialling 999, or the non-emergency line 101, and to your employer.

Call Crimestoppers on 0800 555 111 if you have any information about truck crime or any other crime. Your call is free. You do not have to give your name. You may receive a reward.

ANNEX 8: USEFUL CONTACTS

Further to this Department for Transport guidance, advice on security and other matters can also be obtained from the following organisations:

Health & Safety Executive
http://www.hse.gov.uk/cdg/manual/index.htm

Centre for the Protection of National Infrastructure
www.cpni.gov.uk/help

National Counter Terrorism Security Office
www.gov.uk/government/organisations/national-counter-terrorism-security-office

Security Industry Authority (Security Officer licensing issues only)
www.sia.homeoffice.gov.uk

Home Office
CAST Centre for Applied Science and Technology (research and testing)
Sandridge
St. Albans Hertfordshire AL4 9HQ
Tel 01727 816400
Fax 01727 816 233
Email cast@homeoffice.gsi.gov.uk
Website www.homeoffice.gov.uk

Office for Nuclear Regulation
Cross ONR Programme – Transport
Building 4NG - Redgrave Court
Merton Road
Bootle
Merseyside
L20 7HS
Tel 0151 951 3266
E-mail class7@onr.gsi.gov.uk
Website www.onr.org.uk

British Coatings Federation Ltd
Riverbridge House
Guildford Road
Leatherhead
Surrey
KT22 9AD
Tel 01372 365989
Website www.bcf.co.uk

British Compressed Gas Association
4A Mallard Way, Pride Park
Derby
DE24 8GX
Tel 01332 225120
Fax 01332 225101
E-mail admin@bcga.co.uk
Website www.bcga.co.uk

British International Freight Association
Redfern House
Browells Lane
Feltham
Middlesex
TW13 7EP
Tel 020 8844 2266
E-mail bifa@bifa.org
Website www.bifa.org

Chemical Business Association
Group House Southmere Court, Electra Way
Crewe Business Park
Crewe
Cheshire
CW1 6GU
Tel 01270 258200
Fax 01270 258444
E-mail cba@chemical.org
Website www.chemical.org.uk

Chemical Industries Association
Kings Building, Smith Square
London
SW1P 3JJ
Tel 020 7834 3399
Fax 020 7834 4469
E-mail enquiries@cia.org.uk
Website www.cia.org.uk

Federation of Petroleum Suppliers
Vienna House, International Square, Starley Way
Birmingham International Park
Solihull
B37 7GN
Tel 0121 767 1320
E-mail office@fpsonline.co.uk
Website www.fpsonline.co.uk

Freight Transport Association
Hermes House, St John's Road
Tunbridge Wells
Kent
TN4 9UZ
Tel 01892 526171
Fax 01892 534989
E-mail enquiries@fta.co.uk
Website www.fta.co.uk

National Chemicals Emergency Centre
Gemini Building, Fermi Avenue
Harwell
Didcot
Oxfordshire
OX11 0QR
Tel 01235 753654
Fax 01235 753656
E-mail ncec@ricardo-aea.com
Website www.the-ncec.com

Road Haulage Association
The Old Forge, South Road
Weybridge
Surrey
KT13 9DZ
Tel 01932 841515
E-mail weybridge@rha.uk.net
Website www.rha.uk.net

UKLPG
Camden House
Warwick Road
Kenilworth
Warwickshire
CV8 1TH
E-mail mail@uklpg.org
Website www.uklpg.org

UK Petroleum Industry Association Ltd
Quality House, Quality Court, Chancery Lane
London
WC2A 1HP
Tel 020 7269 7600
E-mail info@ukpia.com
Website www.ukpia.com